SOLUTIONACCELERATORS

Act faster. Go further.

Windows Server® 2008 Security Guide

Security Compliance Management Toolkit

Version 3.0

Published: February 2008 | Updated: February 2009

For the latest information, please see
microsoft.com/wssg

Microsoft

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user's particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

Overview

Welcome to the *Windows Server 2008 Security Guide*. This guide provides instructions and recommendations to help strengthen the security of computers running Windows Server® 2008 that are members of an Active Directory® domain.

In addition to the guidance that the *Windows Server 2008 Security Guide* prescribes, this Solution Accelerator provides tools, step-by-step procedures, recommendations, and processes that significantly streamline the deployment process. This guide not only provides you with effective security setting guidance. It also provides you with a reproducible method that you can use to apply the guidance to both test and production environments.

In order to create, test, and deploy the security settings for either the EC environment or the SSLF environment, you must first run the Windows® Installer (.msi) file for the GPOAccelerator tool that accompanies the download for this toolkit. You can then use this tool to automatically create all the GPOs for the security settings this guide recommends. For instructions about how to use the tool to accomplish these tasks, see the companion document *How to Use the GPOAccelerator*, which is part of the same download. You can also use the Microsoft Excel® workbook Windows Server 2008 Security Baseline Settings that accompanies this guide to compare and evaluate the Group Policy settings.

Microsoft engineering teams, consultants, support engineers, partners, and customers have reviewed and approved this prescriptive guidance to make it:

- **Proven**. Based on field experience.
- **Authoritative**. Offers the best advice available.
- **Accurate**. Technically validated and tested.
- **Actionable**. Provides the steps to success.
- **Relevant**. Addresses real-world security concerns.

Microsoft has published security guides for Windows Server 2003 and Windows 2000 Server. This guide references significant security enhancements in Windows Server 2008. The guide was developed and tested with computers running Windows Server 2008 joined to a domain that uses Active Directory® Domain Services (AD DS).

As the operating system continues to evolve through future releases, you can expect updated versions of this guidance to include more security enhancements. Solution Accelerators are also available to assist you with the deployment and operation of Windows Server 2008. For more information about all available Solution Accelerators, visit Solution Accelerators on TechNet.

Executive Summary

IT security is everybody's business. Every day, adversaries are attempting to invade your networks and access your servers to bring them down, infect them with viruses, or steal information about your customers or employees. Attacks come from all directions: from onsite employee visits to Web sites infected with malware, to offsite employee connections through virtual private networks (VPNs), branch office network connections to corporate servers, or direct assaults on vulnerable computers or servers in your network. Organizations of all sizes now also face more complex and demanding audit requirements.

You know firsthand how essential your servers are to keeping your organization up and running. The data they house and the services they provide are your organization's lifeblood. It is your job to stand guard over these essential assets, prevent them from going down or falling victim to attacks from outside and inside your organization, and to prove to auditors that you have taken all reasonable steps to secure your servers.

Windows Server 2008 is engineered from the ground up with security in mind, delivering an array of new and improved security technologies and features that provide a solid foundation for running and building your business. The *Windows Server 2008 Security Guide* is designed to further enhance the security of the servers in your organization by taking full advantage of the security features and options in Windows Server 2008.

This guide builds on the *Windows Server 2003 Security Guide*, which provides specific recommendations about how to harden servers running Windows Server 2003 Service Pack 2 (SP2). The *Windows Server 2008 Security Guide* provides recommendations to harden servers that use security baselines for the following two environments:

- **Enterprise Client (EC)**. Servers in this environment are located in a domain that uses AD DS and communicate with other servers running Windows Server 2008 or Windows Server 2003 SP2 or later. The client computers in this environment include a mixture: some run Windows Vista® SP1 whereas others run Windows XP Professional SP3 or later. For information about the baseline security settings that this environment uses, see the Windows Server 2008 Security Baseline Settings workbook.
- **Specialized Security – Limited Functionality (SSLF)**. Concern for security in this environment is so great that a significant loss of functionality and manageability is acceptable. For example, military and intelligence agency computers operate in this type of environment. The servers in this environment run only Windows Server 2008. For information about the SSLF settings that this environment uses, see the Windows Server 2008 Security Baseline Settings workbook.

⚠**Caution** The guidance in this chapter positions your organization to establish the SSLF environment, which is distinct from the EC environment. The SSLF guidance is for high security environments only. It is not a supplement to the guidance on the EC environment. Security settings prescribed for the SSLF environment limit key functionality across the environment. For this reason, the SSLF security baseline is not intended for most organizations. Be prepared to extensively test the SSLF security baseline before implementing it in a production environment.

The organization of the guide enables you to easily access the information that you require. The guide and its associated tools help you to:

- Establish and deploy either of the security prescribed baselines in your network environment.
- Identify and use Windows Server 2008 security features for common security scenarios.
- Identify the purpose of each individual setting in either security baseline and understand their significance.

You will need to run the .msi file for the GPOAccelerator tool that accompanies the download for this toolkit to create, test, and deploy the security settings for either the EC environment or the SSLF environment. This tool automatically creates all the GPOs for the security settings this guide recommends. For instructions about how to use the tool to accomplish these tasks, see *How to Use the GPOAccelerator*.

This guide is designed primarily for enterprise customers. To obtain the most value from this material, you will need to read the entire guide. However, it is possible to read individual portions of the guide to achieve specific aims. The "Chapter Summaries" section in this overview briefly introduces the information in the guide. For further information about security topics and settings related to Windows Server 2008, see the Windows Server 2008 Security Baseline Settings workbook and the companion guide, *Threats and Countermeasures*.

After deploying the appropriate security settings across your enterprise you can verify that the settings are in effect on each computer using the *Security Compliance Management Toolkit*. The toolkit includes Configuration Packs that match the recommendations in this guide for the EC and SSLF environments. The toolkit can be used with the Desired Configuration Management (DCM) feature in Configuration Manager 2007® (SP1) to efficiently monitor compliance. In addition, you can quickly and easily run reports to demonstrate how your organization is meeting important compliance regulations. For further information about the toolkit, see *Security Compliance Management Toolkit* on TechNet.

Who Should Read This Guide

The *Windows Server 2008 Security Guide* is primarily for IT professionals, security specialists, network architects, computer engineers, and other IT consultants who plan application or infrastructure development and deployments of Windows Server 2008 for servers in an enterprise environment. The guide is not intended for home users. This guide is for individuals whose jobs may include one for more of the following roles:

- **Security specialist**. Users in this role focus on how to provide security across computing platforms within an organization. Security specialists require a reliable reference guide that addresses the security needs of every level of the organization and also offers proven methods to implement security countermeasures. Security specialists identify security features and settings, and then provide recommendations on how their customers can most effectively use them in high risk environments.
- **IT operations, help desk, and deployment staff**. Users in IT operations focus on integrating security and controlling change in the deployment process, whereas deployment staff focuses on administering security updates quickly. Staff in these roles also troubleshoot security issues related to applications that involve how to install, configure, and improve the usability and manageability of software. They monitor these types of issues to define measurable security improvements and a minimum of impact on critical business applications.
- **Network architect and planner**. Users in this role drive the network architecture efforts for computers in their organizations.
- **Consultant**. Users in this role are aware of security scenarios that span all the business levels of an organization. IT consultants from both Microsoft Services and partners take advantage of knowledge transfer tools for enterprise customers and partners.

Note Users who want to apply the prescriptive guidance in this guide must, at a minimum, read and complete the steps to establish the EC environment in *How to Use the GPOAccelerator*.

Skills and Readiness

The following knowledge and skills are required for consultants, operations, help desk and deployment staff, and security specialists who develop, deploy, and secure server systems running Windows Server 2008 in an enterprise organization:

- MCSE on Microsoft Windows Server 2003 or a later certification and two or more years of security-related experience, or equivalent knowledge.
- In-depth knowledge of the organization’s domain and Active Directory environments.
- Experience with the Group Policy Management Console (GPMC).
- Experience in the administration of Group Policy using the GPMC, which provides a single solution for managing all Group Policy–related tasks.
- Experience using management tools including Microsoft Management Console (MMC), Gpupdate, and Gpresult.
- Experience using the Security Configuration Wizard (SCW).
- Experience deploying applications and server computers in enterprise environments.

Guide Purpose

The primary purposes of this guide are to enable you to do the following:

- Use the solution guidance to efficiently create and apply tested security baseline configurations using Group Policy.
- Understand the reasoning for the security setting recommendations in the baseline configurations that the guide prescribes, and their implications.
- Identify and consider common security scenarios, and then use specific security features in Windows Server 2008 to help you manage them in your environment.
- Understand role based security for different workloads in Windows Server 2008.

The guide is designed to enable you to use only the relevant parts of it to meet the security requirements of your organization. However, readers will gain the most benefit by reading the entire guide.

Guide Scope

This guide focuses on how to help create and maintain a secure environment for servers running Windows Server 2008. The guide explains the different stages of how to secure two different environments, and what each security setting addresses for the servers deployed in either one. The guide provides prescriptive information and security recommendations.

Client computers in the EC environment can run either Windows XP Professional SP3 or later, or Windows Vista SP1. However, the servers that manage these client computers on the network must run Windows Server 2008 or Windows Server 2003 SP2 or later. Client computers in the SSLF environment can only run Windows Vista SP1 and the servers that manage them can only run Windows Server 2008.

This guide includes chapters that provide security recommendations about how to harden the following server roles and the role services that they provide:

- Active Directory Domain Services (AD DS)
- Dynamic Host Configuration Protocol (DHCP) Server
- Domain Name System (DNS) Server
- Web Server (IIS)
- File Services
- Print Services
- Active Directory Certificate Services (AD CS)
- Network Policy and Access Services
- Terminal Services

Note Configuration information about how to set up a server role, such as step-by-step configuration guidance on specific roles, is not in scope for this guide. This guide only includes the security settings available in the operating system that it recommends. However, more configuration information for Windows Server 2008 is available on the *Windows Server 2008 Step-by-Step Guides* Web page on the Microsoft Download Center.

Hardening recommendations for the following server roles are not included in this guide:

- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- Fax Server
- Hyper-V
- Streaming Media Services
- UDDI Services

- Windows Deployment Services

For a thorough discussion of all the security settings in Windows Server 2008, refer to the companion guide, *Threats and Countermeasures*.

Guidance and Tool Requirements

This Solution Accelerator includes the following documents and workbooks:

- *Windows Server 2008 Security Guide*
- Windows Server 2008 Attack Surface Reference workbook
- Windows Server 2008 Security Baseline Settings workbook

  Note The Windows Server 2008 Security Baseline Settings workbook provides CCE unique identifiers for each setting. You can use the CCE identifiers to facilitate fast and accurate correlation of configuration data across multiple information sources and tools.

After downloading the *Windows Server 2008 Security Guide* Solution Accelerator from the Microsoft Download Center, extract these resources on your computer in a location of your choice. You must run the .msi file for the GPOAccelerator tool that accompanies the download for this toolkit to create, test, and deploy the security settings for the *Windows Server 2008 Security Guide*.

Chapter Summaries

This release of the *Windows Server 2008 Security Guide* consists of 11 chapters that you can use to reference setting descriptions, considerations, and values. The Windows Server 2008 Security Baseline Settings workbook that accompanies the guide provides another resource that you can use to compare and evaluate the Group Policy settings. In addition, the Windows Server 2008 Attack Surface Reference workbook provides summary information about services, files, and firewall rules specific to each server role that the guide covers. The following figure shows the guide structure to help inform you how to optimally implement and deploy the prescriptive guidance.

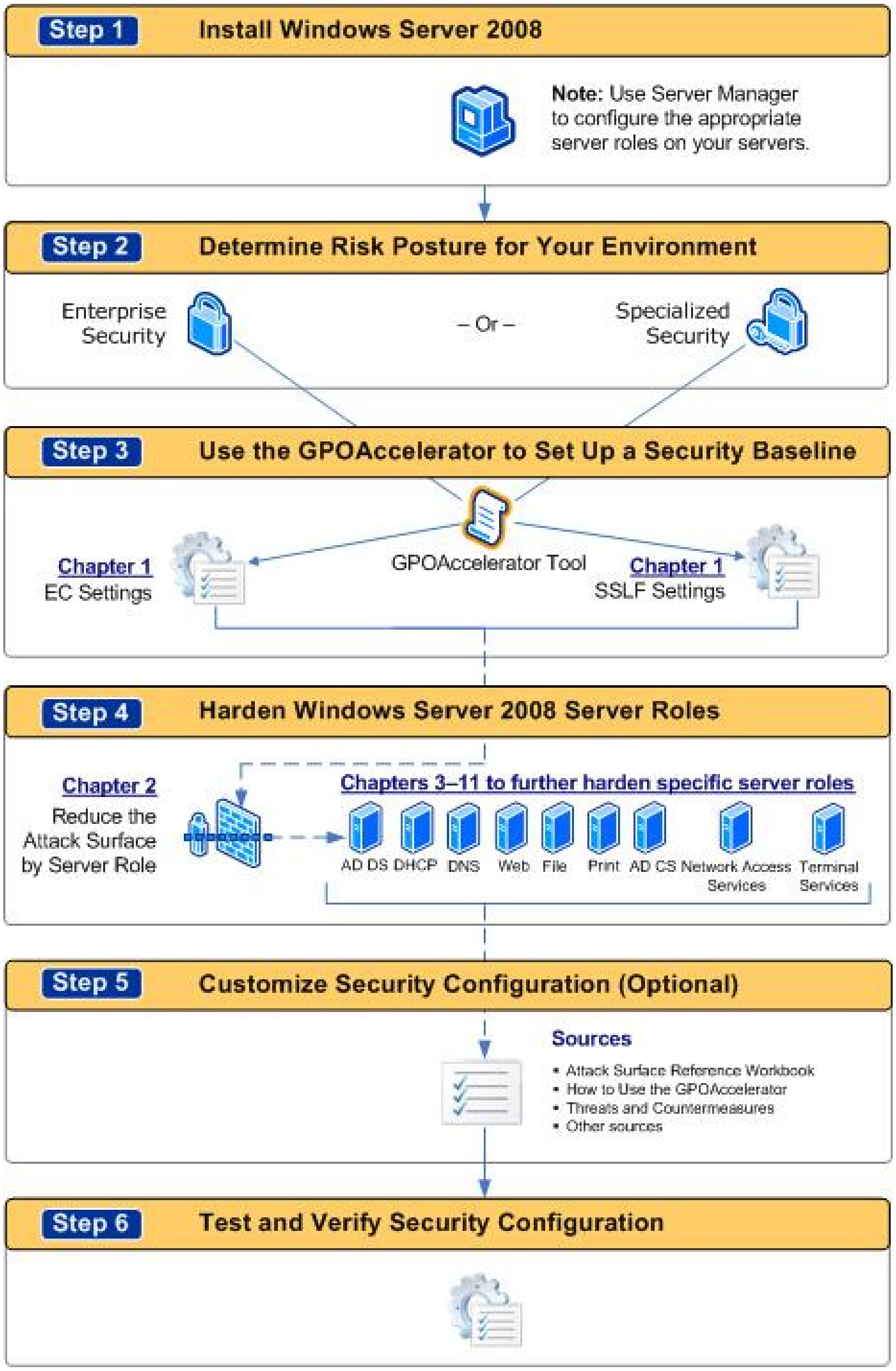

Step 1
Install Windows Server 2008
Note: Use Server Manager to configure the appropriate server roles on your servers.
Step 2
Determine Risk Posture for Your Environment
Enterprise Security
– Or –
Specialized Security
Step 3
Use the GPOAccelerator to Set Up a Security Baseline
Chapter 1
EC Settings
GPOAccelerator Tool
Chapter 1
SSLF Settings
Step 4
Harden Windows Server 2008 Server Roles
Chapter 2
Reduce the Attack Surface by Server Role
Chapters 3–11 to further harden specific server roles
AD DS
DHCP
DNS
Web
File
Print
AD CS
Network Access Services
Terminal Services
Step 5
Customize Security Configuration (Optional)
Sources
• Attack Surface Reference Workbook
• How to Use the GPOAccelerator
• Threats and Countermeasures
• Other sources
Step 6
Test and Verify Security Configuration

Figure 1 Security Guide Structure

Overview

The overview states the purpose and scope of the guide, defines the guide audience, and indicates the organization of the guide to assist you in locating the information relevant to you. It also describes the tools and templates that accompany the guide, and the user prerequisites for the guidance. Brief descriptions follow for each chapter and the appendix for the guide.

Chapter 1: Implementing a Security Baseline

This chapter identifies the benefits to an organization of creating and deploying a security baseline. The chapter includes high-level security design recommendations that you can follow in preparation to implement either the EC baseline settings or the SSLF baseline settings. The chapter explains important security considerations for both the EC environment and the SSLF environment, and the broad differences between these environments.

The Windows Server 2008 Security Baseline Settings workbook that accompanies this guide provides another resource that you can use to compare and evaluate the Group Policy settings. Run the .msi file for the GPOAccelerator tool that accompanies the download for this toolkit to create, test, and deploy the security settings for either the EC environment or the SSLF environment. For instructions on how to use the tool, see *How to Use the GPOAccelerator*.

⚠**Caution** The guidance in this chapter positions your organization to establish the SSLF environment, which is distinct from the EC environment. The SSLF guidance is for high security environments only. It is not a supplement to the guidance on the EC environment. Security settings prescribed for the SSLF environment limit key functionality across the environment. For this reason, the SSLF security baseline is not intended for most organizations. Be prepared to extensively test the SSLF security baseline before implementing it in a production environment.

Chapter 2: Reducing the Attack Surface by Server Role

This chapter provides an overview of built-in tools in Windows Server 2008 that can help you to quickly configure, maintain, and enforce all of the required functionality for the servers in your environment. The chapter discusses using Server Manager to help reduce the attack surface of your servers by only configuring the functionality that each specific server role requires.

The chapter then discusses how you can use the Security Configuration Wizard (SCW) to help maintain and enforce the configuration implemented by Server Manager. The chapter also provides information about Server Core, a new installation option in Windows Server 2008.

Chapter 3: Hardening Active Directory Domain Services

This chapter discusses how organizations can harden Active Directory Domain Services (AD DS) to manage users and resources, such as computers, printers, and applications on a network. AD DS in Windows Server 2008 includes a number of new features that are not available in previous versions of Windows Server®, and some of these features focus on deploying AD DS more securely. Features that enhance security in AD DS include new auditing capabilities, fine-grained password policies, and the ability to use read-only domain controllers (RODCs).

Chapter 4: Hardening DHCP Services

This chapter provides prescriptive guidance for hardening the DHCP Server role. The chapter discusses DHCP Server and DHCP Client services in Windows Server 2008 that include security-related enhancements for Network Access Protection (NAP) and DHCPv6 functionality.

Chapter 5: Hardening DNS Services

This chapter provides prescriptive guidance for hardening the DNS Server role. Windows Server 2008 provides enhancements in the DNS Server service that focus on improving performance or provide new features, including background zone loading to help circumvent potential denial-of-service (DoS) attacks, and support for RODCs located in perimeter networks, branch offices, or other unsecured environments.

Chapter 6: Hardening Web Services

This chapter provides prescriptive guidance for hardening the Web Server role. The chapter discusses how the Web server role installs Microsoft® Internet Information Services (IIS) 7.0, which has been redesigned into forty modular components that you can choose to install as needed.

Chapter 7: Hardening File Services

This chapter provides prescriptive guidance for hardening the File Server role. File servers can provide a particular challenge to harden, because balancing security and functionality of the fundamental services that they provide is a fine art. Windows Server 2008 introduces a number of new features that can help you control and harden a file server in your environment.

Chapter 8: Hardening Print Services

This chapter provides prescriptive guidance for hardening the Print Server role. Significant security changes were introduced to printing services in the operating system for Windows Vista, and these changes have also been incorporated into Windows Server 2008 for your organization to take full advantage of them.

Chapter 9: Hardening Active Directory Certificate Services

This chapter provides prescriptive guidance for hardening Active Directory Certificate Services (AD CS) on a server running Windows Server 2008. AD CS provides customizable services for creating and managing public key certificates used in software security systems that employ public key technologies. The chapter discusses how your organizations can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding private key.

Chapter 10: Hardening Network Policy and Access Services

This chapter provides prescriptive guidance for hardening Network Policy and Access Services on servers running Windows Server 2008. Network Policy and Access Services (NPAS) in Windows Server 2008 provide technologies that allow you to deploy and operate a virtual private network (VPN), dial-up networking, 802.1x protected wired and wireless access, and Cisco Network Admission Control (NAC)-based devices.

The chapter discusses how you can use NPAS to define and enforce policies for network access authentication, authorization, as well as client health using Network Policy Server (NPS), the Routing and Remote Access Service, Health Registration Authority (HRA), and the Host Credential Authorization Protocol (HCAP).

Chapter 11: Hardening Terminal Services

This chapter provides prescriptive guidance for hardening Terminal Services on servers running Windows Server 2008. These servers provide essential services that allow users to access Windows-based programs or the full Microsoft Windows® desktop from various locations. Windows Server 2008 includes a number of specific role services for this technology that your organization can use, including TS Licensing to manage Terminal Server client access licenses (TS CALS) that are required for devices and users to connect to a terminal server.

The chapter also discusses how the Terminal Services Session Broker (TS Session Broker) role service supports reconnection to an existing session on a terminal server that is a member of a load-balanced terminal server farm, how the Terminal Services Gateway (TS Gateway) role service enables authorized users to connect to terminal servers and remote desktops on the corporate network over the Internet using RDP via HTTPS, and how the Terminal Services Web Access (TS Web Access) role service allows authorized users to gain access to terminal servers via a Web browser.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this guide on Microsoft.com:

- Infrastructure Planning and Design.
- Microsoft Assessment and Planning Toolkit.
- Microsoft Deployment.
- *Microsoft Windows Security Resource Kit*.
- *Microsoft Windows Server 2003 Resource Kit*.
- Security Guidance.
- Solution Accelerators.
- *Threats and Countermeasures*.
- *Windows Server 2003 Security Guide*.
- Windows XP TechCenter.
- *Windows XP Security Guide*.

Feedback

The Solution Accelerators – Security and Compliance (SA–SC) team would appreciate your thoughts about this and other solution accelerators.

Please send your comments using the following resources:

- E-mail to: secwish@microsoft.com.

We look forward to hearing from you.

Acknowledgements

The Solution Accelerators – Security and Compliance (SA–SC) team would like to acknowledge and thank the team that produced the *Windows Server 2008 Security Guide*. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Development Team

Authors and Experts

Benjamin Curry – *Content Master*

Kurt Dillard – *kurtdillard.com*

Richard Harrison – *Content Master*

Byron Hynes – *Microsoft*

Doug Steen – *Wadeware LLC*

Developers

Bhakti Bhalerao – *Infosys Technologies Ltd*

Haikun Zhang – *Minesage Co Ltd*

Hui Zeng – *Minesage Co Ltd*

José Maldonado – *Microsoft*

Michael Tan – *Microsoft*

Naresh Krishna Kumar Kulothungan – *Infosys Technologies Ltd*

ZhiQiang Yuan – *Minesage Co Ltd*

Editors

John Cobb – *Wadeware LLC*

Steve Wacker – *Wadeware LLC*

Product Managers

Alain Meeus – *Microsoft*

Jim Stuart – *Microsoft*

Shruti Kala – *Microsoft*

Program Manager

Vlad Pigin – *Microsoft*

Release Manager

Karina Larson – *Microsoft*

Test Managers

Gaurav Singh Bora – *Microsoft*

Sumit Parikh – *Microsoft*

Testers

Ankit Agarwal – *Infosys Technologies Ltd*

Beenu Venugopal – *Infosys Technologies Ltd*

Dhanashri Dorle – *Infosys Technologies Ltd*

Raxit Gajjar – *Infosys Technologies Ltd*

Swaminathan Viswanathan – *Infosys Technologies Ltd*

Contributors and Reviewers

Sreenivas Addagatla, Starr Anderson, Brandon Baker, Siddharth Bhai, Daniel H. Brown, Derick Campbell, Chase Carpenter, Pankaj Chhabra, Richard Costleigh, Raf Cox, Jan Decrock, Ido Dubrawsky, Nils Dussart, Thomas Deml, Pitchai "Elango" Elangom, Lambert Green, Roger Grimes, Jim Groves, Robert Hoover, Manu Jeewani, Dan Kaminsky, David Kennedy, David Kruse, Nazim Lala, Anthony Leibovitz, Richard Lewis, Adrian Lannin, Greg Lindsay, Brad Mahugh, Aaron Margosis, Greg Marshall, Georgi Matev, Herbert Mauerer, Nathan Muggli, Doug Neal, Ramasubramanian K. Neelmani, Marco Nuijen, Chandra Nukala, Frank Olivier, Ashwin Palekar, Sanjay Pandit, Abhishek Pathak, Enrique Saggese, Oded Ye Shekel, Michiko Short, Eugene Siu, Jeff Westhead, and Sudarshan Yadav, John Addeo (Dimension Data America), Jorge de Almeida Pinto (MVPS), Renato Miguel de Barros (Modulo Security Solutions), Jan De Clercq (Hewlett-Packard), Guido Grillenmeier (Hewlett-Packard), Jakob H. Heidelberg (Interprise Consulting A/S), Korean Government, Juergen Otter (Siemens AG), Vern Perryman (Hewlett-Packard), Stephan Reitinger (Siemens AG Austria), Derek Seaman (PointBridge), Alex Vandurme (NCIRC/NATO), David Vanophalvens (NCIRC/NATO), and Werner Kraus (Siemens AG Austria).

Note The United States Department of Commerce National Institute of Standards and Technology (NIST) participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.

Note At the request of Microsoft, the National Security Agency Information Assurance Directorate participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.

Chapter 1: Implementing a Security Baseline

Windows Server® 2008 is the most secure operating system that Microsoft has produced to date. However, every organization needs to consider what level of security and functionality is required. Therefore, you may need to make specific configuration changes to meet the requirements of your environment. This chapter demonstrates how relatively easy it is to configure security settings to harden computers that perform different server roles. Each server is running Windows Server 2008 in the default configuration and is joined to a domain using Active Directory® Domain Services (AD DS).

You can now harden the default operating system using only Group Policy objects (GPOs). Previous guidance from Microsoft required importing Security Template .inf files and extensive manual modification of the Administrative Templates portion of several GPOs. Working with these files and templates is no longer necessary. However, the Security Template .inf files are included with the GPOAccelerator tool so that you can use them to harden stand-alone servers. A "stand-alone" server is not a member of an AD DS domain. All of the recommended Group Policy settings are documented in the Windows Server 2008 Security Baseline Settings workbook that accompanies this guide.

To deploy this guidance, you need to:

- Create an organizational unit (OU) structure for your environment.
- Run the GPOAccelerator tool for this guide.

  Important You must run the .msi file for the GPOAccelerator tool that accompanies the download for this toolkit to create, test, and deploy the security settings for the *Windows Server 2008 Security Guide*. This tool automatically creates all the GPOs for the security settings this guide recommends. The tool also includes Security Template .inf files that you can use to apply security settings to stand-alone servers.
- Use the Group Policy Management Console (GPMC) to link and manage the GPOs.

⚠**Caution** It is essential to thoroughly test your OU and GPO designs before deploying them in a production environment. For procedural details about how to accomplish this, see *How to Use the GPOAccelerator*. Use this guidance to create and deploy the OU structure and security GPOs during both the test and production phases of the implementation.

The security baseline GPOs for this guide provide a combination of tested settings that enhance security for computers running Windows Server 2008 in the following two distinct environments:

- **Enterprise Client (EC)**
- **Specialized Security – Limited Functionality (SSLF)**

Enterprise Client Environment

The Enterprise Client (EC) environment referred to in this chapter consists of a domain using AD DS in which computers running Windows Server 2008 with Active Directory manage client computers that can run either Windows Vista® Service Pack 1 (SP1) or Windows XP® Professional (SP3) or later, and member servers running Windows Server 2008 or Windows Server 2003 SP2 or later. The client computers and member servers are managed in this environment through Group Policy, which is applied to sites, domains, and OUs. Group Policy provides a centralized infrastructure within AD DS that enables directory-based change and configuration management of user and computer settings, including security and user data.

Note The Enterprise Client (EC) security baseline this guide prescribes helps to provide enhanced security that allows sufficient functionality of the operating system and applications for the majority of organizations.

Specialized Security – Limited Functionality Environment

The Specialized Security – Limited Functionality (SSLF) environment referred to in this chapter consists of a domain using AD DS in which computers running Windows Server 2008 with Active Directory manage client computers that can run either Windows Vista® Service Pack 1 (SP1) or Windows XP® Professional SP3 or later, and member servers running Windows Server 2008.

The Specialized Security – Limited Functionality (SSLF) baseline for this guide addresses the demand to help create highly secure environments for computers running Windows Server 2008. Concern for security is so great in these environments that a significant loss of functionality and manageability is acceptable. These setting recommendations have been developed in cooperation with several government agencies from around the world.

⚠**Caution** The SSLF security settings are not intended for the majority of enterprise organizations. The configuration for these settings has been developed for organizations where security is more important than functionality.

If you decide to test and deploy the SSLF configuration settings to servers in your environment, the IT resources in your organization may experience an increase in help desk calls related to the limited functionality that the settings impose. Although the configuration for this environment provides a higher level of security for data and the network, it also prevents some services from running that your organization may require. Examples of this include Terminal Services, which allows users to connect interactively to desktops and applications on remote servers.

It is important to note that the SSLF baseline is not an addition to the EC baseline: the SSLF baseline provides a distinctly different level of security. For this reason, do not attempt to apply the SSLF baseline and the EC baseline to the same computers. Rather, for the purposes of this guide, it is imperative to first identify the level of security that your environment requires, and then decide to apply either the EC baseline or the SSLF baseline. You can use the Windows Server 2008 Security Baseline Settings workbook that accompanies this guide provides to compare setting values.

Important If you are considering whether to use the SSLF baseline for your environment, be prepared to exhaustively test the computers in your environment after you apply the SSLF security settings to ensure that they do not prohibit required functionality for the computers in your environment.

Specialized Security

Organizations that use computers and networks, especially if they connect to external resources such as the Internet, must address security issues in system and network design, and how they configure and deploy their computers. Capabilities that include process automation, remote management, remote access, availability 24 hours a day, worldwide access, and software device independence enable businesses to become more streamlined and productive in a competitive marketplace. However, these capabilities also expose the computers of these organizations to potential compromise.

In general, administrators take reasonable care to prevent unauthorized access to data, service disruption, and computer misuse. Some specialized organizations, such as those in the military, government, and finance are required to protect some or all of the services, systems, and data that they use with a specialized security level. The SSLF baseline is designed to provide this level of security for these organizations. To preview the SSLF settings, see the Windows Server 2008 Security Baseline Settings workbook that accompanies this guide.

Limited Functionality

The specialized security the SSLF baseline implements may reduce functionality in your environment. This is because the SSLF baseline limits users to only the specific functions that they require to complete necessary tasks. Access is limited to approved applications, services, and infrastructure environments. There is a reduction in configuration functionality because the baseline disables many property pages with which users may be familiar.

The following sections in this chapter describe the areas of higher security and limited functionality that the SSLF baseline enforces:

- Restricted services and data access.
- Restricted network access.
- Strong network protection.

Restricted Services and Data Access

Specific settings in the SSLF baseline can prevent valid users from accessing services and data by requiring strong passwords that users can more easily forget or misspell. In addition, these settings may lead to an increase in help desk calls. However, the security benefits that the settings provide help make it harder for malicious users to attack computers running Windows Server 2008 in this environment. Setting options in the SSLF baseline that could potentially prevent users from accessing services and data include those that:

- Restrict administrative groups such as Backup Operators and Server Operators.
- Enforce stronger password requirements.
- Require more strict account lockout policy.
- Require more strict **User Rights Assignments** and **Security Options** policy.

Note The Windows Server 2008 Security Baseline Settings workbook that accompanies this guide provides another resource that you can use to compare setting values of the EC and the SSLF baselines.

Group Policy can either restrict or enforce the default setting values of many user rights and security options. This can cause some applications that require specific user rights on a computer to not function properly. For this reason, it is important to closely review user right and security option setting requirements for applications that are outside the realm of those that are installed for different server roles. These can include but are not limited to applications developed specifically for your environment or tools used to perform diagnostics or updates for your computers.

Restricted Network Access

Network reliability and system connectivity is paramount for successful business. Microsoft operating systems provide advanced networking capabilities that help to connect systems, maintain connectivity, and repair broken connections. Although this capability is beneficial to maintaining network connectivity, attackers can use it to disrupt or compromise the computers on your network.

Administrators generally welcome features that help to support network communications. However, in special cases, the primary concern is the security of data and services. In such specialized environments, some loss of connectivity is tolerated to help ensure data protection. Setting options in the SSLF baseline that increase network security but could potentially prevent users from network access include those that:

- Limit access to client systems across the network.
- Hide systems from browse lists.
- Control Windows Firewall exceptions.
- Implement connection security, such as packet signing.

Strong Network Protection

A common strategy to attack network services is to use a denial of service (DoS) attack. Such an attack prevents connectivity to data or services or overextends system resources and degrades performance. The SSLF baseline provides additional protections to system objects and the assignment of resources to help guard against this type of attack. Setting options in the SSLF baseline that help to prevent DoS attacks include those that control:

- Process memory quota assignments.
- Object creation.
- The ability to debug programs.
- Process profiling.

All of these security considerations contribute to the possibility that the security settings in the SSLF baseline may prevent applications in your environment from running or users from accessing services and data as expected. For these reasons, it is important to extensively test the SSLF baseline after you implement it and before you deploy it in a production environment.

Security Design

The security design that this chapter recommends forms the starting point for the scenarios in this guide, as well as the mitigation suggestions for the scenarios. The remaining sections in this chapter provide design details about the core security structure for the guide:

- **OU Design for Security Policies**
- **GPO Design for Security Policies**

OU Design for Security Policies

An OU is a container within an AD DS domain. An OU may contain users, groups, computers, and other OUs. If an OU contains other OUs, it is called a parent OU, and an OU within a parent OU is called a child OU.

You can link a GPO to an OU, which will then apply the GPO's settings to the users and computers that are contained in that OU and its child OUs. And to facilitate administration, you can delegate administrative authority for each OU to specific administrators or groups.

OUs provide an effective way to segment administrative boundaries for users and computers. Microsoft recommends that organizations assign users and computers to separate OUs, because some settings only apply to users and other settings only apply to computers.

You can delegate control over an individual OU by using the Delegation Wizard in the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in tool. See the "More Information" section at the end of this chapter for links to documentation about how to delegate authority.

One of the primary goals of an OU design for any environment is to provide a foundation for a Group Policy implementation that can apply to all computers in the AD DS domain. This helps ensure that the computers meet the security standards set by your organization. The OU design must also provide an adequate structure to accommodate security settings for specific types of server roles, role services, and users in an organization. For example, developers may require access to their computers that average users do not. The following figure illustrates a simple OU structure that is sufficient for the Group Policy discussion in this chapter. The OU structure may differ from the requirements for your organization's environment.

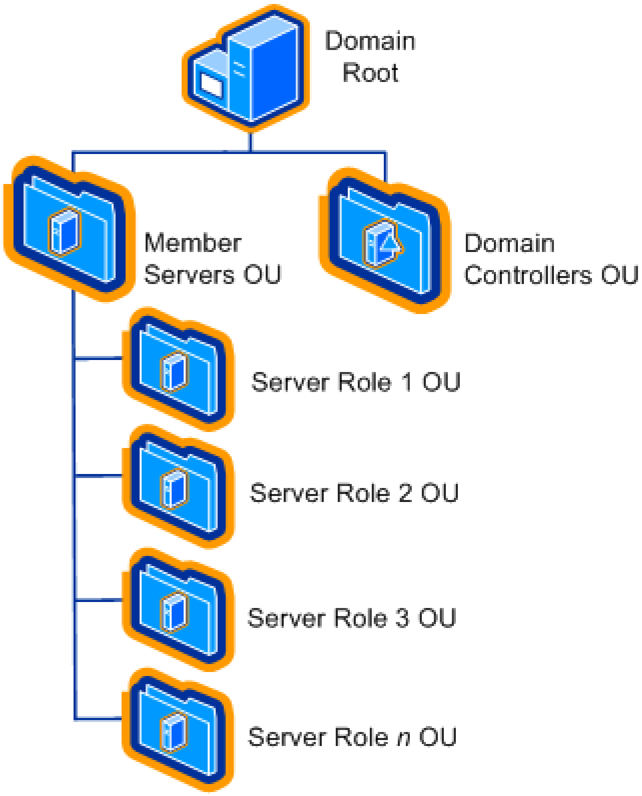


Figure 1.1 Example OU structure for computers running Windows Server 2008

Domain Root

You should apply some security settings throughout the domain to control how the domain, as a whole, is configured. These settings are contained in GPOs that apply to the domain. Computers and Users are not managed in this container.

Domain Controllers OU

Domain controllers hold some of the most sensitive data in your organization — data that controls the security configuration itself. You apply GPOs at this level in the OU structure to configure and protect the domain controllers.

Member Servers OU

This OU contains child OUs as described below. You should include settings that apply to all servers, but not to workstations, in the GPOs that you apply to this OU.

Server Role OUs

Microsoft recommends creating an OU for each server role that your organization uses. Each OU should contain only one type of server computer. You can then configure GPO settings and apply them to OUs that are specific to each role.

You can also choose to combine certain roles on the same server, if your organization requires it. For example, you may choose to combine the File and Print server roles. In this case, you can create an OU for these combined server roles called "File and Print Server," and then link the two role-specific GPO policies to that OU.

Important Combining server roles on the same computer requires careful planning and testing to ensure that you do not negatively affect the overall security of the server roles that you combine.

GPO Design for Security Policies

A GPO is a collection of Group Policy settings. GPOs are stored at the domain level and affect users and computers contained in sites, domains, and OUs.

You can use GPOs to ensure that specific policy settings, user rights, and computer behavior apply to computers or users in an OU. Using Group Policy instead of a manual configuration process makes it simple to manage and update changes for many computers and users. Manual configuration is not only inefficient, because it requires a technician to visit each workstation, but it is also potentially ineffective. This is primarily because if the policy settings in domain-based GPOs are different than those applied locally, the domain-based GPO policy settings will overwrite the locally applied policy settings.

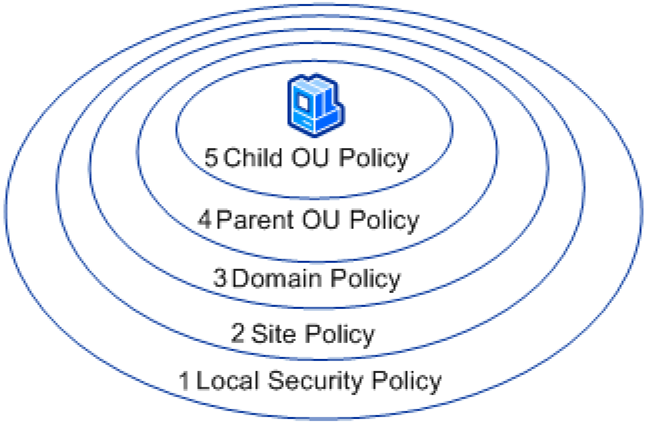


Figure 1.2 GPO order of precedence

The previous figure shows the order of precedence in which GPOs are applied to a computer that is a member of the Child OU, from the lowest priority (1) to the highest priority (5). Group Policy is applied first from the local security policy of each workstation. After the local security policy is applied, GPOs are next applied at the site level, and then at the domain level.

For computers running Windows Server 2008, Windows Server 2003 SP2 or later, and Windows Vista SP1 or Windows XP Professional SP3 or later that are nested in several OU layers, GPOs are applied in order from the parent OU level in the hierarchy to the lowest child OU level. The final GPO is applied from the OU that contains the computer account. This order of GPO processing for Group Policy—local security policy, site, domain, parent OU, and child OU—is significant because settings in GPOs that are applied later in the process will overwrite settings applied earlier. Different values for the same setting configured in different GPOs are never combined. User GPOs are applied in the same manner.

The following considerations apply when you design Group Policy:

- An administrator must set the order in which you link multiple GPOs to an OU, or Group Policy will be applied by default in the order it was linked to the OU. If the same setting is configured in multiple policies, the policy that is highest on the policy list for the container will take precedence.
- Group Policy settings apply to users and computers based on where the user or computer object is located in Active Directory. In some cases, you may need to apply policy to user objects based on the location of the computer object. The Group Policy loopback feature gives administrators the ability to apply user Group Policy settings based on which computer the user is logged on to. For more information about this topic, see the "Loopback Processing of Group Policy" article.
- You may configure a GPO with the **Enforced** option. If you select this option, other GPOs cannot override the settings that are configured in this GPO.
- In Active Directory, you may configure a site, domain, or an OU with the **Block policy inheritance** option. This option blocks GPO settings from GPOs that are higher in the Active Directory hierarchy unless they have the **Enforced** option selected. In other words, the **Enforced** option has precedence over the **Block policy inheritance** option.

  Note Administrators should only use the **Enforced** option and the **Block policy inheritance** option with utmost care because enabling these options can make troubleshooting GPOs difficult and cumbersome.

Recommended GPOs

To implement the OU design described above requires a minimum of the following GPOs:

- A policy for the domain.
- A policy to provide the baseline security settings for all domain controllers.
- A policy to provide the baseline security settings for all member servers.
- A policy for each server role in your organization.

Note Additional GPOs are required to implement security for client computers and users in your organization. For more information, see the *Windows Vista Security Guide*.

The following figure expands on the preliminary OU structure to show the linkage between these GPOs and the OU design.

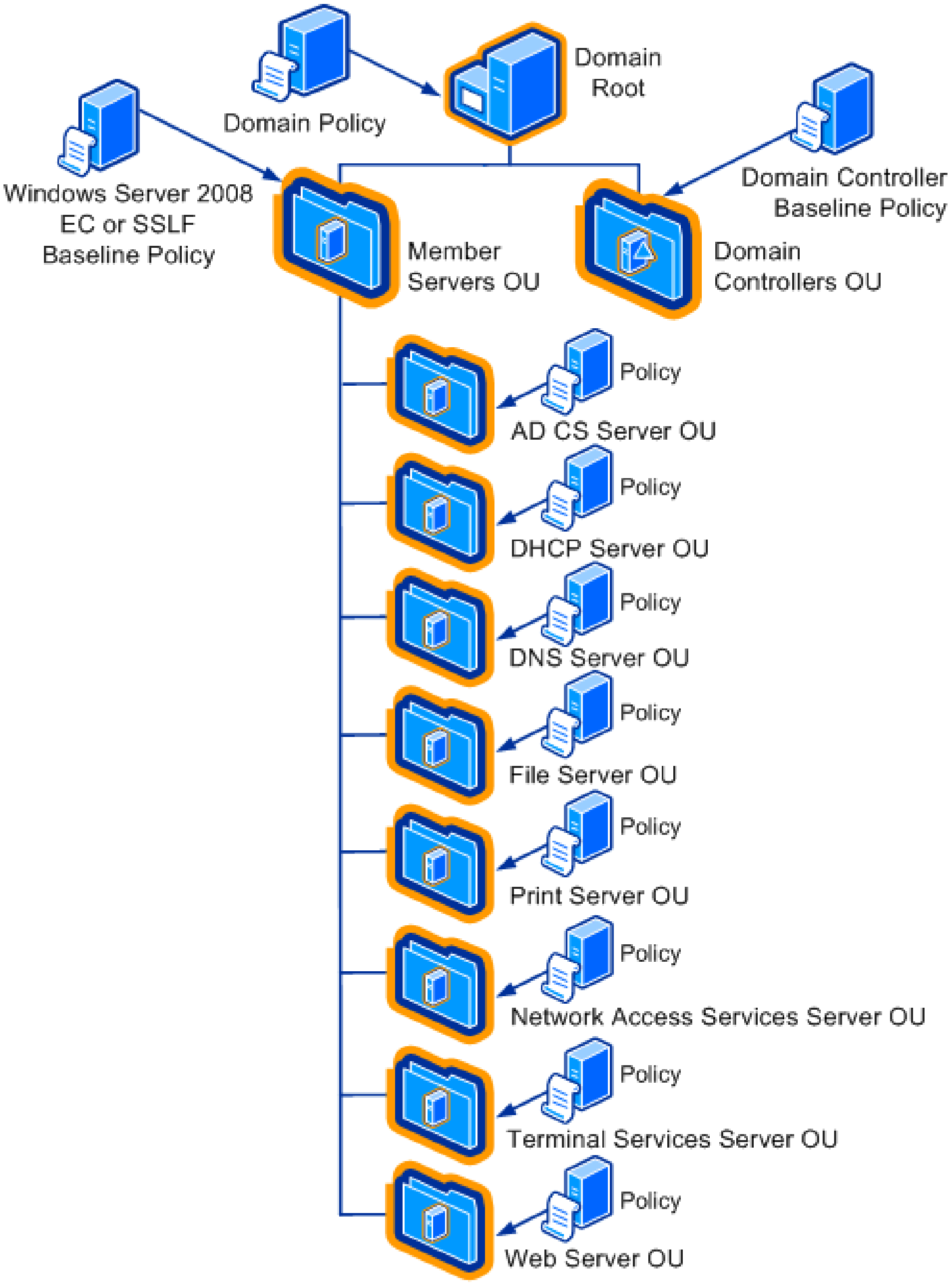


Figure 1.3 Example OU structure and GPO links for computers running Windows Server 2008

In the example in Figure 1.3, a File server is a member of the File Server OU. The first policy that is applied to the server is the local security policy. However, in general, little if any configuration of the servers is done by local policy. Security policies and settings should always be enforced by Group Policy.

Because there is only one File server in this example, no GPOs are applied at this level, which leaves the Domain GPO as the next policy that is applied to the servers. The Windows Server 2008 EC Baseline Policy is then applied to the Member Servers OU. Finally, any specific polices for the Web servers in the environment are applied to the Web Server OU.

As a precedence example, consider a scenario in which the policy setting for **Allow logon through Terminal Services** is set to apply to the following OUs and user groups:

- Member Servers OU – **Administrators** group
- Web Server OU – **Remote Desktop Users** and **Administrators** groups

In this example, logon through Terminal Services has been restricted to the **Administrators** group for servers in the Member Servers OU. However, a user whose account is in the **Remote Desktop Users** group can log on to a File server through Terminal Services because the File Servers OU is a child of the Member Servers OU and the child policy takes precedence.

If you enable the **Enforced** policy option in the GPO for the Member Servers OU, only users with accounts in the **Administrators** group can log on to the File server computer through Terminal Services. This is because the **Enforced** option prevents the child OU policy from overwriting the policy applied earlier in the process.

More Information

The following resources provide additional information about Windows Server 2008 security-related topics on Microsoft.com:

- Administering Group Policy.
- Enterprise Management with the Group Policy.
- Loopback Processing of Group Policy.
- Migrating GPOs Across Domains with GPMC.
- *Step-by-Step Guide for Microsoft Advanced Group Policy Management 3.0*.
- *Step-by-Step Guide to Using the Delegation of Control Wizard*.
- Summary of New or Expanded Group Policy.
- Tasks and Tools on the Update Management Center for managing updates.
- Windows Server 2008 TechCenter.
- Windows Server Group Policy.
- *Windows Vista Security Guide*.

Chapter 2: Reducing the Attack Surface by Server Role

The concept of server roles is not new, but the ability to centralize server role management is a new feature that is at the core of Windows Server® 2008. Aside from basic network connectivity, a default installation of Windows Server 2008 does not provide any services to the network. The operating system's secure-by-default design requires administrators to enable all desired functionality as a part of any server deployment.

This chapter provides an overview of built-in tools that can help you quickly configure, maintain, and enforce all of the required functionality for the servers in your environment.

- The "Securing Server Roles" section reviews how you can use the Server Manager Microsoft Management Console (MMC) snap-in to help reduce the attack surface of your servers by only configuring the functionality that each specific server role requires.
  - This section also introduces the Server Core feature of Windows Server 2008, which can help you further reduce the attack surface of the server roles in your organization.
  - This section also discusses how you can use the Security Configuration Wizard (SCW) to help maintain and enforce the configuration that you implemented using Server Manager.
- The "Using SCW and Group Policy to Improve Security" section provides guidance about how to create and apply Group Policy objects (GPOs) to harden servers that run Windows Server 2008.

Securing Server Roles

The Server Manager MMC in Windows Server 2008 eases the task of managing and securing multiple server roles in an organization. Server Manager provides a single source for managing a server's identity and system information, displaying server status, identifying problems with server role configuration, and managing all roles installed on the server. After you establish a secure server configuration, you can use the SCW to help ensure that the servers remain configured as intended.

Server Manager

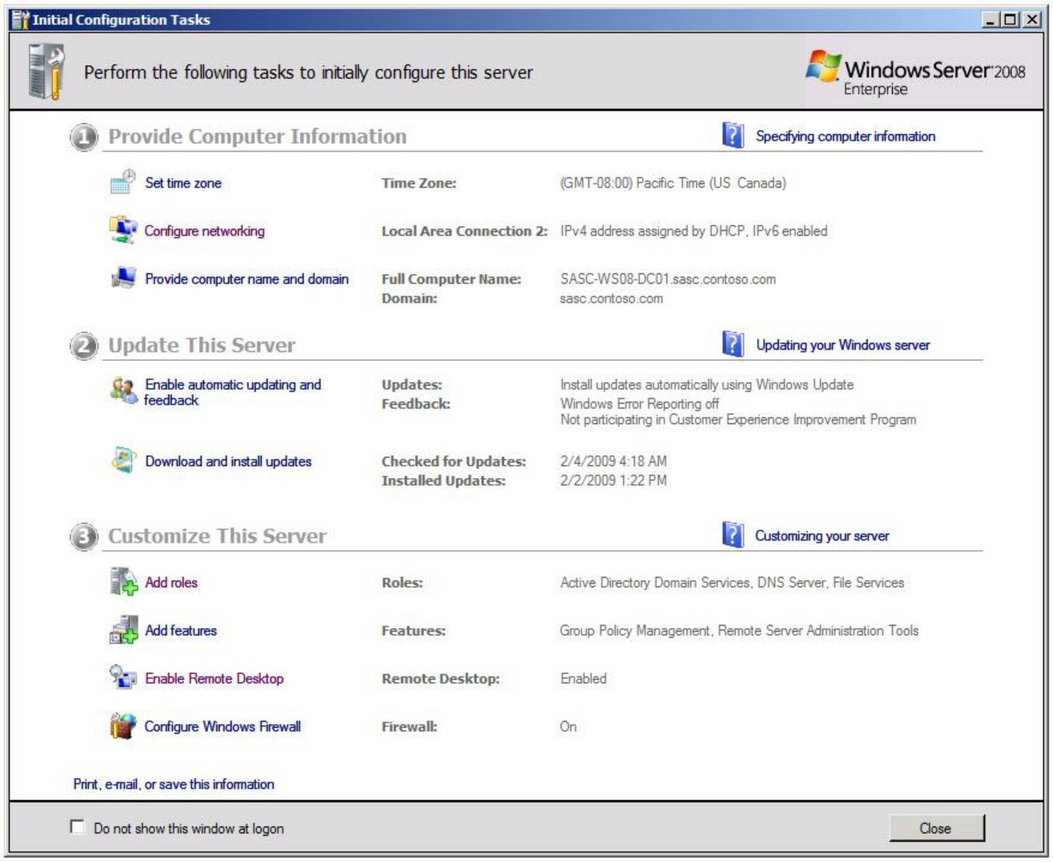
Server Manager accelerates server setup and configuration, and simplifies the ongoing management of server roles. In Windows Server 2008, each server role is dedicated to performing a different primary server function. You can dedicate a server to perform a single role, or choose to install multiple server roles on one server. For example, the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) roles are often installed on one server.

However, server features that are optionally installed to support functionality and add security do not usually describe a server's primary function. For example, Microsoft® BitLocker™ Drive Encryption is a feature that you can install on a file server or any other server role. This feature can help protect the data on a server if it is stolen.

Server Manager replaces several features included with Windows Server® 2003, including Manage Your Server, Configure Your Server, and Add or Remove Windows Components. Server Manager also eliminates the requirement that you run the SCW before deploying servers. When you use Server Manager in Windows Server 2008 to install server roles, the roles are configured with Microsoft-recommended security settings by default. You can also use the SCW to help enforce the proper configuration of server roles on your servers.

The default installation of Windows Server 2008 runs a minimal number of services and no server roles or features. This design helps protect each newly installed server role by minimizing the attack surface of each server as much as possible.

You must configure the proper server roles on the servers in your environment before they can perform any useful functions. Server Manager includes the Initial Configuration Tasks (ICT) feature, which automatically displays when an administrator logs on to a new server for the first time, as shown in the following figure.



Initial Configuration Tasks

Perform the following tasks to initially configure this server

1 Provide Computer Information — Specifying computer information

Set time zone — Time Zone: (GMT-08:00) Pacific Time (US Canada)

Configure networking — Local Area Connection 2: IPv4 address assigned by DHCP, IPv6 enabled

Provide computer name and domain — Full Computer Name: SASC-WS08-DC01.sasc.contoso.com
Domain: sasc.contoso.com

2 Update This Server — Updating your Windows server

Enable automatic updating and feedback — Updates: Install updates automatically using Windows Update
Feedback: Windows Error Reporting off
Not participating in Customer Experience Improvement Program

Download and install updates — Checked for Updates: 2/4/2009 4:18 AM
Installed Updates: 2/2/2009 1:22 PM

3 Customize This Server — Customizing your server

Add roles — Roles: Active Directory Domain Services, DNS Server, File Services

Add features — Features: Group Policy Management, Remote Server Administration Tools

Enable Remote Desktop — Remote Desktop: Enabled

Configure Windows Firewall — Firewall: On

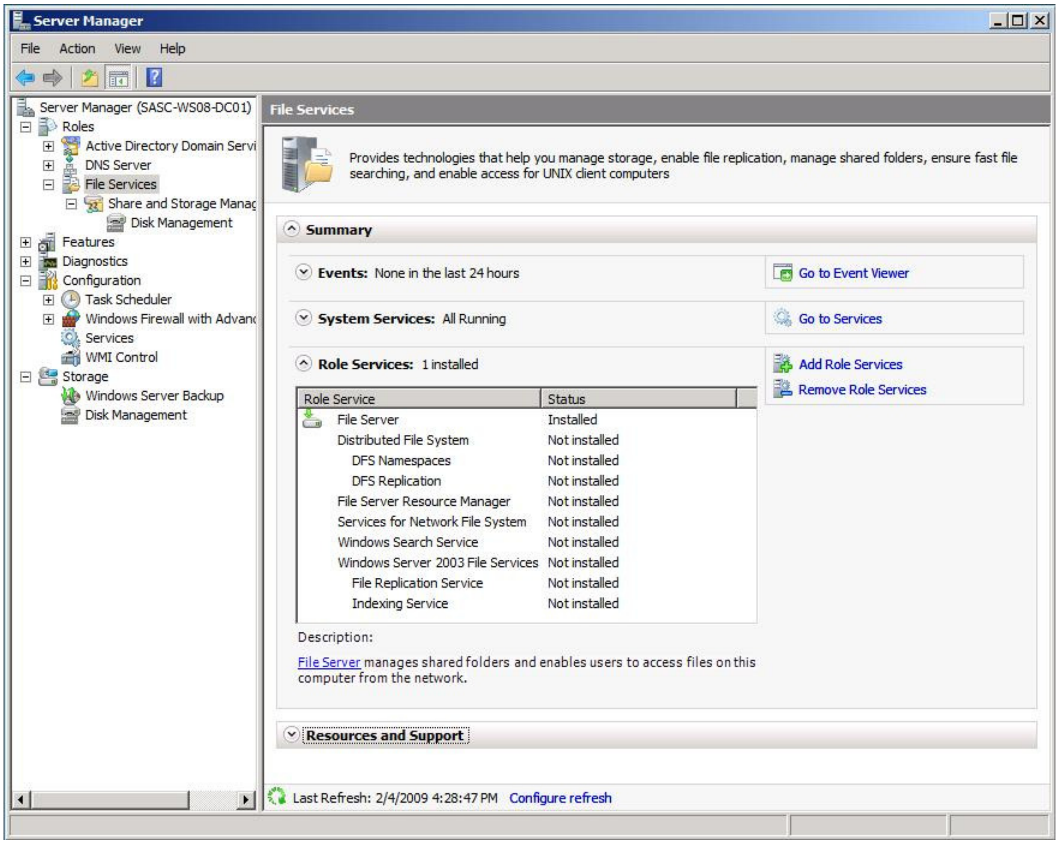
Print, e-mail, or save this information

☐ Do not show this window at logon

Figure 2.1 The Initial Configuration Tasks (ICT) feature in Server Manager

The ICT highlights and organizes important tasks for administrators to complete on all new server installations by helping them quickly access the most commonly used configuration wizards in Server Manager.

You can normally accomplish the configuration and customization of each server using Server Manager, which you can access by running ServerManager.msc or by clicking the Server Manager shortcut that is pinned by default to the Start menu.



Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

Events: None in the last 24 hours

System Services: All Running

Role Services: 1 installed

Role Service	Status
File Server	Installed
Distributed File System	Not installed
DFS Namespaces	Not installed
DFS Replication	Not installed
File Server Resource Manager	Not installed
Services for Network File System	Not installed
Windows Search Service	Not installed
Windows Server 2003 File Services	Not installed
File Replication Service	Not installed
Indexing Service	Not installed

Description:

File Server manages shared folders and enables users to access files on this computer from the network.

Last Refresh: 2/4/2009 4:28:47 PM

Figure 2.2 The Server Manager console

When configuring a role, Server Manager automatically installs all required services and features. Server Manager also automatically configures any firewall rules that are required to support the new role. Similarly, when you use Server Manager to remove any specific role, the server's services and firewall configuration are modified to help ensure that the server's configuration remains secure, and that the operation of other server roles is not affected. These modifications help ensure that the server only runs required services and that it maintains a minimal attack surface.

The server role chapters in this guide include information about all installed services and the open ports that each server role uses. Also, the Server Manager page on Microsoft TechNet provides detailed technical information about Server Manager and the server roles that it supports.

Server Core

Server Core is a new installation option in Windows Server 2008. Server Core helps reduce the attack surface of the supported server roles by installing only a subset of the binary files that a server requires to operate. This approach also reduces the size of the server installation, which helps reduce the number of files that might require updates in the future. For example, the Explorer shell and Microsoft Internet Explorer® cannot be installed as part of a Server Core installation.

A Server Core installation supports the following server roles:

- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- DNS Server
- DHCP Server
- File Services
- Print Services
- Streaming Media Services
- Web Server (IIS)
- Hyper-V™

The following optional features are also supported:

- Microsoft Failover Cluster
- Network Load Balancing
- Subsystem for UNIX-based Applications
- Windows Backup
- Multipath I/O
- Removable Storage Management
- BitLocker Drive Encryption
- Simple Network Management Protocol (SNMP)
- Windows Internet Naming Service (WINS)
- Telnet client
- Quality of Service (QoS)

Server Core requires only about 1 GB of space on the server's hard disk drive to install, and an additional 2 GB for normal operations. After installing and configuring the server, you can manage it either locally from a command prompt, remotely by using Remote Desktop, or by using the MMC or command-line tools that support remote use. When applicable, the server role chapters in this guide point out when a Server Core installation can help you better secure your environment.

For detailed information and guidance about how to install Server Core, see the *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide* on TechNet.

Security Configuration Wizard

The Security Configuration Wizard (SCW) functionality in Windows Server 2008 is similar to the functionality in the Windows Server 2003 Service Pack 2 (SP2) version of the wizard. You can still use the SCW to reduce the attack surface of a server by disabling unneeded services and blocking unused or unnecessary ports. However, using the wizard is now an optional process.

Windows Server 2003 was designed for administrators to use the SCW after installing a default version of the operating system on a server to reduce its attack surface. However, now when you install Windows Server 2008 on a computer, Server Manager automatically determines what is needed on the server and implements the minimum functionality required for the server to fulfill its specific role.

The SCW uses a step-by-step approach that guides you through different aspects of the configuration process that you can analyze and then optimally configure. The SCW is not an MMC snap-in, but a self-contained program that you can access by running SCW.exe.

You can use the SCW to rapidly create security policies for multiple servers or groups of servers from a single computer. This capability allows you to manage policies throughout the organization from a single location. These policies provide consistent, supported hardening measures that are appropriate for the functions that each server provides within the organization.

The SCW is integrated with the new Windows Firewall in Windows Server 2008. Unless you prevent it from doing so, the SCW will configure Windows Firewall to permit inbound network traffic to important ports that the operating system requires as well as listening applications. If additional port filters are required, you can use the SCW to create them. As a result, policies that the SCW creates address the need for custom scripts to set or modify IPsec filters to block unwanted traffic. This capability simplifies the management of network hardening. You also can use the SCW to simplify the configuration of network filters for services that use remote procedure call (RPC) or dynamic ports.

For more information about the new Windows Firewall, see the article "The New Windows Firewall in Windows Vista and Windows Server 2008" on TechNet.

It is no longer necessary to run the SCW to reduce the attack surface of individual servers. However, you can still take advantage of the SCW to create and deploy security policies that you can use to help maintain a configuration implemented by Server Manager across one or more servers using Group Policy.

When you use the SCW to create a new policy, it uses the current configuration of a server as an initial configuration. Therefore, it is best to create the policy on a server that is the same server type as the one for which you are creating the policy. This approach will streamline the task somewhat because the starting configuration should approximately match the desired configuration. When you use the SCW to create a new policy, it creates an XML file and saves it in the %systemdir%\security\msscw\Policies folder by default. After you create your policies, you can use either the SCW or the SCWcmd.exe command-line tool to apply the policies directly to your test servers.

The next section in this chapter focuses on how to use the SCW and SCWcmd.exe to create GPOs to help enforce your server security configuration. For more detailed information about the SCW, including the wizard's capabilities and links to other SCW resources, see the "Security Configuration Wizard Concepts" page on TechNet.

Using SCW and Group Policy to Improve Security

You can use the SCW to create and apply security policies directly to servers. However, this approach would be a time-consuming process for a large number of servers. Microsoft recommends to deploy SCW policies using the SCWcmd.exe tool to convert the SCW XML–based policy into a GPO, which you can then apply to a large number of servers at one time. Although at first this conversion might seem an unnecessary step, this approach provides the following advantages:

- Familiar Active Directory–based mechanisms replicate, deploy, and apply the policies.
- GPOs that are made available to you through this conversion allow you to incrementally use policies with organizational units (OUs) and policy inheritance to fine-tune the hardening of similarly configured servers that are not exactly the same. For example, with Group Policy you can place servers in a child OU and then apply an incremental policy. If you use the SCW for this task, you must create a new policy for each unique configuration in your environment.
- The policies are automatically applied to all servers that are placed in corresponding OUs. If you use the SCW, you must either manually apply the policies or use a customized scripting solution.

Using the SCW to Create Role Policies

Use a new installation of the operating system to start your configuration work. This approach helps ensure that there are no legacy settings or software from previous configurations that could interfere with your work. If possible, use hardware that is similar to the hardware for your deployment to help ensure as much compatibility as possible. In the following procedure, the new installation is called a reference computer.

To create a role policy

1. Create a new installation of Windows Server 2008 on a new reference computer.
2. Use the ICT tool to join the computer to the domain.
3. Install mandatory applications on your reference computer. Such applications could include software and management agents, tape backup agents, and antivirus or antispyware utilities.
4. Use Server Manager to install the appropriate server roles. For example, if your target servers will run DHCP and DNS, install those roles.

   Note You do not have to configure each workload exactly the same way on the servers that you deploy, but you must install the roles so that the SCW can determine the proper configuration of each server.
5. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Security Configuration Wizard**.
6. On the **Configuration Action** page, select **Create new policy**, and then click **Next**.
7. On the **Select Server** page, type the name or IP address of the reference computer, and then click **Next**.

   Note This action enters the local computer name by default.
8. On the **Processing Security Configuration Database** page, click **Next**, and then on the **Role-Based Service Configuration** page, click **Next**.

9. On the **Select Server Roles** page, ensure that the wizard has detected and selected all of the installed server roles on your reference computer. Then click **Next**.

   Caution If the wizard does not select all of the roles that you want to install on the server, the resulting policy will disable services that some roles require, and the server will not operate properly.

10. On the **Select Client Features** page, ensure that the wizard has detected and selected all of the installed features on your reference computer. Then click **Next**.

    Caution If the wizard does not select all of the features that you want to install on the server, the resulting policy will disable services that some roles require, and the server will not operate properly.

11. On the **Select Administration and Other Options** page, ensure that the wizard has detected and selected all of the installed options on your reference computer. Then click **Next**.
12. On the **Select Additional Services** page, ensure that the wizard has detected and selected all of the required services on your reference computer. Then click **Next**.

    Note If you have configured your reference computer with all required roles and installed any additional required software, such as backup agents or antivirus software, you should not need to modify any of the previous Role-based Service Configuration pages.

13. On the **Handling Unspecified Services** page, click **Next**.
14. On the **Confirm Service Changes** page, review the service mode changes that the SCW will include in the resulting security policy, and then click **Next**.

    Caution Pay close attention to any services whose startup mode changes from Automatic to Disabled to ensure that you do not disable any required functionality.

15. On the **Network Security** page, click **Next**.
16. On the **Network Security Rules** page, ensure that the SCW has detected the appropriate ports and applications it will use to configure Windows Firewall. Then click **Next**.
17. On the **Registry Settings** page, select the **Skip this section** checkbox, and click **Next**.
18. On the **Audit Policy** page, select the **Skip this section** checkbox, and click **Next**.
19. On the **Save Security Policy** page, click **Next**.
20. On the **Security Policy File Name** page, specify the appropriate path, name the policy to save it, and then click **Next**.

    Note By default, the XML–based policy files are saved to the Security\msscw\policies folder under the server's installation folder (typically this is located at C:\Windows). However, the SCW allows you to specify another location.

21. On the **Apply Security Policy** page, click the **Apply Later** option, and then click **Next**.

    Note You can select the **Apply Now** option to apply the security policy directly to a server. This allows you to apply a security policy to stand-alone servers.

22. Finally, on the **Completing the Security Configuration Wizard** page, click **Finish**.

The following procedure guides you through using SCWcmd.exe to convert the XML–based SCW policy file that you just created into a GPO.

To convert a role policy into a GPO

1. At a command prompt, type the following, and then press ENTER:

```
scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>
```

The following example creates a GPO named File Server Policy in Active Directory. You must specify a unique name for the new GPO, or the command will return an error:

```
scwcmd transform
/p:"C:\Windows\Security\msscw\Policies\FileServer.xml"
/g:"File Server Policy"
```

Note This example displays on multiple lines because of display limitations and to make it easier to read. However, you must type the information at the command prompt on one line when you run the command.

2. Use the Group Policy Management Console (GPMC) to link the newly created GPO to the appropriate OUs.
3. The GPOAccelerator tool mentioned in Chapter 1, "Implementing a Security Baseline," creates example GPOs that were originally created using the SCW. These example GPOs have been modified to not disable any system services and to not implement any firewall rules. While this allows you to combine these GPOs for servers configured to perform multiple roles, the GPOs only serve to ensure that required system services remain enabled.
4. While this provides a mechanism to help ensure system availability, an ideal GPO also disables any services that are not required. You can use the GPOs created by the GPOAccelerator tool on your production servers, but considerable benefit is gained by creating GPOs specifically tailored to your servers using the previous procedures.

Important You must run the .msi file for the GPOAccelerator tool that accompanies the download for this toolkit to create, test, and deploy the security settings for the *Windows Server 2008 Security Guide*. This tool automatically creates all the GPOs for the security settings this guide recommends. The tool also includes Security Template .inf files that you can use to apply security settings to stand-alone servers.

Domain Policy Settings

A relatively small number of security settings are applied to the domain. These settings are applied through the Computer Configuration node in the Group Policy Object Editor. Within this node, the following setting groups appear in the Windows Settings sub-node:

- Password Policy Settings
- Account Lockout Policy Settings

This section provides an overview of these two categories of settings, for information about which specific settings are recommended for each role review the Microsoft Excel® workbook Windows Server 2008 Security Baseline Settings that accompanies this guide. For detailed information about how each setting functions, what threats each addresses, and the potential consequences of using each setting read the companion guide, *Threats and Countermeasures*.

Password Policy Settings

Complex passwords that you change regularly help reduce the likelihood of a successful password attack. Password policy settings control the complexity and lifetime of passwords. Generally, you configure password policy settings only by using Group Policy at the domain level.

Note Windows Server 2008 supports a new feature called Fine-Grained Password Policies that provides organizations with a way to define different password and account lockout policies for different sets of users in a domain. In Windows® 2000 and Windows Server® 2003 Active Directory® domains, only one password policy and account lockout policy could be applied to all users in the domain. This guide does not make recommendations for this feature. For more information about Fine-Grained Password Policies, see the AD DS: Fine-Grained Password Policies page on Microsoft TechNet.

You can configure the password policy settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Account Lockout Policy Settings

The account lockout policy is an Active Directory Domain Services (AD DS) security feature that locks a user account. The lock prevents logon after a specified number of failed logon attempts occur within a specified period. Domain controllers track logon attempts, and the number of allowed attempts based on values that are configured for the account lockout settings. In addition, you can specify the duration of the lock.

These policy settings help prevent attackers from guessing user passwords, and they decrease the likelihood of successful attacks on your network environment. However, an enabled account lockout policy will probably result in more support issues for network users. Before you enable the following settings, ensure that your organization wants to accept this additional management overhead. For many organizations, an improved and less-costly solution is to automatically scan the Security event logs for domain controllers and generate administrative alerts when it appears that someone is attempting to guess passwords for user accounts.

You can configure the account lockout policy settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Domain Controller and Member Server Policy Settings

The majority of the security settings are applied to domain controllers and member servers in the domain. Many recommendations are the same for both domain controllers and member servers. However, some settings apply only to domain controllers. These settings are applied through the Computer Configuration node in the Group Policy Object Editor. Within this node, these settings appear in the Windows Settings and Administrative Templates sub-nodes.

If you compare the recommendations for some settings between domain controllers and member servers, you may notice some cases where the recommended value for domain controllers is "Not defined." This is because some settings are configured in the built-in Group Policy called "Default Domain Controller Policy." When the default values for such settings match the recommendations for domain controllers in the Enterprise Client environment, the recommended value is listed as "Not defined" in the Microsoft Excel® workbook Windows Server 2008 Security Baseline Settings that accompanies this guide.

However, a specific value for member servers may be recommended for the same setting.

This section provides an overview of the different categories of settings, for information about which specific settings are recommended for each role review the Microsoft Excel® workbook Windows Server 2008 Security Baseline Settings that accompanies this guide. For detailed information about how each setting functions, what threats each addresses, and the potential consequences of using each setting read the companion guide, *Threats and Countermeasures*.

User Rights Assignment Settings

In conjunction with many of the privileged groups in Windows Server 2008, you can assign a number of user rights to specific users or groups. These rights would typically be assigned to perform a specific administrative task or tasks without giving full administrative control to that user or group. To set the value of a user right to **No one**, enable the setting but do not add any users or groups to it. To set the value of a user right to **Not Defined**, do not enable the setting. You can configure the user rights assignment settings in Windows Server 2008 at the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Note Many features in IIS require certain accounts such as IIS_WPG, IIS IUSR_<*ComputerName*>, and IWAM_<*ComputerName*> to have specific privileges. For more information about what user rights are required by accounts that are related to IIS, see IIS and Built-in Accounts (IIS 6.0).

Security Options Settings

The security option settings that are applied through Group Policy on servers in your environment enable or disable capabilities and features such as floppy disk drive access, CD-ROM drive access, and logon prompts. These settings also configure various other settings, such as those for the digital signing of data, administrator and guest account names, and how driver installation works. You can configure the security option settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

MSS Settings

The following settings include registry value entries that do not display by default through the Security Configuration Editor (SCE). These settings, which are all prefixed with MSS:, were developed by the Microsoft Solutions for Security group for previous security guidance. The GPOAccelerator for this guide modifies the SCE so that it properly displays the MSS settings.

User Account Control

User Account Control (UAC) reduces the exposure and attack surface of the operating system by requiring that all users run in standard user mode, even if they have logged on with administrative credentials. This limitation helps minimize the ability for users to make changes that could destabilize their computers or inadvertently expose the network to viruses through undetected malware that has infected the computer. When a user attempts to perform an administrative task, the operating system must raise their security level to allow the task to take place. The UAC settings in GPOs configure how the operating system responds to a request to heighten security privileges.

Potential Issues with SMB Signing Policies

When SMB signing policies are enabled and a Server Message Block (SMB) version 1 client establishes a non-guest session or a non-anonymous session with a server, the client enables security signatures for the server. Later sessions then inherit the security signature sequence that is already established.

To improve security, Windows Server 2008 and Windows Vista SP1 prevent server authenticated connections from being maliciously downgraded to a guest session or to an anonymous session. However, this improved security does not work as intended when the domain controller is running Windows Server 2003 and the client computers are running Windows Vista SP1 or Windows Server 2008. Specifically, this applies if the policies in the following locations are enabled on a domain controller that is running Windows Server 2003 in a domain:

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)

The following policies are enabled on a member computer that is running Windows Vista SP1 or Windows Server 2008 in the same domain:

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (If server agrees)

To download a hotfix to resolve this issue, and learn more about this topic, see "Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled": Microsoft Knowledge Base article 950876.

Event Log Security Settings

The event log records events on the system, and the Security log records audit events. The event log container of Group Policy is used to define attributes that are related to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods. You can configure the event log settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Event Log

Audit Policies and Subcategories

An Audit policy determines which security events to report to administrators to establish a record of user or system activity based on specified event categories. Administrators can monitor security-related activity, such as who accesses an object, when users log on to or log off from computers, or if changes are made to an Audit policy setting. For all of these reasons, Microsoft recommends that you form an Audit policy for an administrator to implement in your environment.

However, before you implement an Audit policy you must investigate which event categories to audit in your environment. The audit settings you choose within the event categories define your Audit policy. Then an administrator can create an Audit policy to meet the security needs of your organization.

If you do not configure audit settings, it will be difficult or impossible to determine what took place during a security incident. However, if you configure audit settings so that too many authorized activities generate events, the Security event log will fill up with too much data. The information in the following sections of this appendix is designed to help you decide what to monitor to facilitate the collection of relevant audit data for your organization.

Windows Server® 2008 includes the same nine Audit policy categories that are present in earlier versions of Windows:

- System
- Logon/Logoff
- Object Access
- Privilege Use
- Detailed Tracking
- Policy Change
- Account Management
- Directory Service Access
- Account Logon

However, Windows Server 2008 allows you to manage Audit policy in a more precise way by including 50 Audit policy subcategories. Although not all subcategories apply to Windows Server 2008–based computers, you can configure many of them to record specific events that provide valuable information.

Configuring Audit Policy Settings

In the past, you could easily configure any of the nine audit categories using Group Policy. Although the same method is possible with Windows Server 2008, you cannot individually configure the new audit subcategories using the Group Policy Management Console (GPMC) because the subcategories are not exposed in the GPMC. If you enable any of the audit category settings in Windows Server 2008 that are present in the GPMC, this action also enables subcategory settings related to each category. For this reason, enabling Audit policy settings by category will likely cause excessive audit logging that will quickly fill up your event logs.

Microsoft recommends to configure only necessary audit subcategory settings using a command-line tool included in Windows Server 2008 called AuditPol.exe.

Using a command-line tool to implement prescribed Audit policy settings across many computers is difficult. However, Microsoft has developed a solution for configuring audit subcategories using Group Policy. The scripts and Group Policy objects (GPOs) included with the security guide automatically implement these settings for you.

When you run the GPOAccelerator as described in Chapter 1, "Implementing a Security Baseline," the script automatically copies the following member server and domain controller files to the NETLOGON share of one of your domain controllers.

For the EC environment:

- EC-WSSGAuditPolicy-MS.cmd
- EC-WSSGApplyAuditPolicy-MS.cmd
- EC-WSSGAuditPolicy-MS.txt
- EC-WSSGAuditPolicy-DC.cmd
- EC-WSSGApplyAuditPolicy-DC.cmd
- EC-WSSGAuditPolicy-DC.txt

For the SSLF environment:

- SSLF-WSSGAuditPolicy-MS.cmd
- SSLF-WSSGApplyAuditPolicy-MS.cmd
- SSLF-WSSGAuditPolicy-MS.txt
- SSLF-WSSGAuditPolicy-DC.cmd
- SSLF-WSSGApplyAuditPolicy-DC.cmd
- SSLF-WSSGAuditPolicy-DC.txt

These files will then automatically replicate to the NETLOGON share of the domain controllers in your domain that uses Active Directory® Domain Services (AD DS). The specific GPOs that the GPOAccelerator creates include a computer startup script that runs these files to configure the prescribed Audit policy settings. The first time these files run on a computer, a scheduled task named WSSGAudit is created. This task will run every hour to help ensure that the Audit policy settings are up to date.

This is the same principle that the *Windows Vista Security Guide* recommends for client computers running Windows Vista. For more information about the solution for configuring new Audit policy settings in Windows Vista in a Windows Server 2003–based domain, see "How to use Group Policy to configure detailed security auditing settings for Windows Vista client computers in a Windows Server 2003 domain or in a Windows 2000 domain": Microsoft Knowledge Base article 921469.

The following tables summarize the Audit policy setting recommendations for servers in the two types of secure environments discussed in the *Windows Server 2008 Security Guide*. Review these recommendations and adjust them as appropriate for your organization. Information about how to modify and remove the Audit policy settings that the GPOs configure appears after the Audit policy setting tables.

Note Microsoft recommends taking extra caution in using Audit settings that can generate large volumes of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategory settings, the high volume of audit events these settings generate will make it difficult to find other types of entries in the Security event log. Such a configuration could also have a significant negative effect on performance.

Audit Policy Subcategories

The following sections provide a brief description of each Audit policy. The tables in each section include recommendations for domain controllers in the two types of secure environments discussed in this guide.

Note Descriptions for each Audit policy subcategory are not provided in this appendix. For additional information on the available Audit policy subcategories and related security events, see

"Description of security events in Windows Vista and in Windows Server 2008": Microsoft Knowledge Base article 947226.

System

The System audit category in Windows Server 2008 allows you to monitor system events that succeed and fail, and provides a record of these events that may help determine instances of unauthorized system access. System events include starting or shutting down computers in your environment, full event logs, or other security-related events that affect the entire system.

The System audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.1 System Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Security System Extension	Success and Failure	Success and Failure	Success and Failure	Success and Failure
§ System Integrity	Success and Failure	Success and Failure	Success and Failure	Success and Failure
§ IPsec Driver	Success and Failure	Success and Failure	Success and Failure	Success and Failure
§ Other System Events	No auditing	No auditing	No auditing	No auditing
§ Security State Change	Success and Failure	Success and Failure	Success and Failure	Success and Failure

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Logon/Logoff

The Logon/Logoff audit category in Windows Server 2008 generates events that record the creation and destruction of logon sessions. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource.

If you configure the **Audit logon events** setting to **No auditing**, it is difficult or impossible to determine which users have accessed or attempted to access your organization's computers.

The Logon/Logoff events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.2 Logon/Logoff Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Logon	Success	Success and Failure	Success	Success and Failure

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Logoff	Success	Success	Success	Success
§ Account Lockout **Note** No events map to this category.	No auditing	No auditing	No auditing	No auditing
§ IPsec Main Mode	No auditing	No auditing	No auditing	No auditing
§ IPsec Quick Mode	No auditing	No auditing	No auditing	No auditing
§ IPsec Extended Mode	No auditing	No auditing	No auditing	No auditing
§ Special Logon	Success	Success	Success	Success
§ Other Logon/Logoff Events	No auditing	No auditing	No auditing	No auditing
§ Network Policy Server	No auditing	No auditing	No auditing	No auditing

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Object Access

By itself, the Object Access audit category in Windows Server 2008 will not audit any events. Settings in this category determine whether to audit when a user accesses an object—for example, a file, folder, registry key, or printer—that has a specified system access control list (SACL), which effectively enables auditing to occur.

Access control entries (ACEs) comprise a SACL. Each ACE contains three pieces of information:

- The security principal (user, computer, or group) to be audited.
- The specific access type to be audited, called an access mask.
- A flag to indicate whether to audit failed access events, successful access events, or both.

If you configure the **Audit object access** setting to **Success**, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to **Failure**, an audit entry is generated each time that a user fails an attempt to access an object with a specified SACL.

Organizations should define only the actions that they want enabled when they configure SACLs. For example, you might want to enable the **Write and Append Data** auditing setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed.

The Object Access events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.3 Object Access Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ File System	No auditing	Failure	No auditing	Failure
§ Registry	No auditing	Failure	No auditing	Failure
§ Kernel Object	No auditing	No auditing	No auditing	No auditing
§ SAM	No auditing	No auditing	No auditing	No auditing
§ Certification Services	No auditing	No auditing	No auditing	No auditing
§ Application Generated	No auditing	No auditing	No auditing	No auditing
§ Handle Manipulation	No auditing	No auditing	No auditing	No auditing
§ File Share	No auditing	No auditing	No auditing	No auditing
§ Filtering Platform Packet Drop	No auditing	No auditing	No auditing	No auditing
§ Filtering Platform Connection	No auditing	No auditing	No auditing	No auditing
§ Other Object Access Events	No auditing	No auditing	No auditing	No auditing

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Configuring and Testing Object Access Audit Rules

The following procedures describe how to configure audit rules on a file or folder, and how to test each audit rule for each object in the specified file or folder.

Note You must use Auditpol.exe to configure the File System subcategory to audit Success and Failure events. Then you can use the following procedure to log events in the Security event log.

To define an audit rule for a file or folder

1. Use Windows Explorer to locate the file or folder and then click it.
2. On the **File** menu, click **Properties**.
3. Click the **Security** tab, and then click the **Advanced** button.
4. Click the **Auditing** tab.
5. If prompted for administrative credentials, click **Continue**, type your username and password, and then press ENTER.
6. Click the **Add** button to make the **Select User, Computer, or Group** dialog box display.
7. Click the **Object Types** button, and then in the **Object Types** dialog box, select the object types you want to find.

   Note The **User, Group, and Built-in security principal** object types are selected by default.

8. Click the **Locations** button, and then in the **Location** dialog box, select either your domain or local computer.
9. In the **Select User or Group** dialog box, type the name of the group or user you want to audit. Then, in the **Enter the object names to select** dialog box, type **Authenticated Users** (to audit the access of all authenticated users) and then click **OK**.

   The **Auditing Entry** dialog box displays.
10. Determine the type of access you want to audit on the file or folder using the **Auditing Entry** dialog box.

    Note Remember that each object access may generate multiple events in the event log and cause it to grow rapidly.
11. In the **Auditing Entry** dialog box, next to **List Folder**/**Read Data**, select **Successful** and **Failed**, and then click **OK**.

    You can view the audit entries you enabled under the **Auditing** tab of the **Advanced Security Settings** dialog box.
12. Click **OK** to close the **Properties** dialog box.

To test an audit rule for a file or folder

1. Open the file or folder.
2. Close the file or folder.
3. Start the Event Viewer. Several Object Access events with Event ID 4663 will appear in the Security event log.
4. Double-click the events as needed to view their details.

Privilege Use

The Privilege Use audit category in Windows Server 2008 determines whether to audit each instance of a user exercising a user right. If you configure these setting values to **Success**, an audit entry is generated each time that a user right is exercised successfully. If you configure these settings values to **Failure**, an audit entry is generated each time that a user right is exercised unsuccessfully. These policy settings can generate a very large number of event records.

The Privilege Use events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.4 Privilege Use Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Sensitive Privilege Use	No auditing	Success and Failure	No auditing	Success and Failure
§ Non Sensitive Privilege Use	No auditing	No auditing	No auditing	No auditing
§ Other Privilege Use Events	No auditing	No auditing	No auditing	No auditing

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Detailed Tracking

The Detailed Tracking audit category in Windows Server 2008 determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. Enabling **Audit process tracking** will generate a large number of events, so it is typically set to **No Auditing**. However, this setting can provide a great benefit during an incident response from information in the log about when processes started and when they were launched.

The Detailed Tracking events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.5 Detailed Tracking Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Process Termination	No auditing	No auditing	No auditing	No auditing
§ DPAPI Activity	No auditing	No auditing	No auditing	No auditing
§ RPC Events	No auditing	No auditing	No auditing	No auditing
§ Process Creation	Success	Success	Success	Success

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Policy Change

The Policy Change audit category in Windows Server 2008 determines whether to audit every incident of a change to user rights assignment policies, Windows Firewall policies, Trust policies, or changes to the Audit policy itself. The recommended settings would let you see any account privileges that an attacker attempts to elevate—for example, if an attacker were to attempt to turn off auditing, that change itself would be recorded.

The Policy Change events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.6 Policy Change Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Audit Policy Change	Success and Failure	Success and Failure	Success and Failure	Success and Failure
§ Authentication Policy Change	Success	Success	Success	Success
§ Authorization Policy Change	No auditing	No auditing	No auditing	No auditing
§ MPSSVC Rule-Level Policy Change	No auditing	No auditing	No auditing	No auditing
§ Filtering Platform Policy Change	No auditing	No auditing	No auditing	No auditing

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Other Policy Change Events	No auditing	No auditing	No auditing	No auditing

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Account Management

The Account Management audit category in Windows Server 2008 helps you track attempts to create new users or groups, rename users or groups, enable or disable user accounts, change account passwords, and enable auditing for Account Management events. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user and group accounts.

The Account Management events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.7 Account Management System Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
User Account Management	Success	Success and Failure	Success	Success and Failure
Computer Account Management	Success	Success and Failure	Success	Success and Failure
Security Group Management	Success	Success and Failure	Success	Success and Failure
Distribution Group Management	No auditing	No auditing	No auditing	No auditing
Application Group Management	No auditing	No auditing	No auditing	No auditing
Other Account Management Events	Success	Success and Failure	Success	Success and Failure

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Directory Service Access

The Directory Service Access audit category in Windows Server 2008 applies only to domain controllers. For this reason, the Directory Service Access audit category and all related subcategories are configured to **No Auditing** for member servers in both environments discussed in the security guide.

The Directory Service Access events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.8 Directory Service Access Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Directory Service Access	Success	Success and Failure	No auditing	No auditing
§ Directory Service Changes	Success	Success and Failure	No auditing	No auditing
§ Directory Service Replication	No auditing	No auditing	No auditing	No auditing
§ Detailed Directory Service Replication	No auditing	No auditing	No auditing	No auditing

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Account Logon

The Account Logon audit category in Windows Server 2008 generates events for credential validation. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on.

The Account Logon events audit category contains subcategories defined in the following table, along with configuration recommendations for each one.

Table 2.9 Account Logon Audit Policy Subcategory Recommendations

Audit policy subcategory	EC domain controller	SSLF domain controller	EC member server	SSLF member server
§ Kerberos Authentication Service	No auditing	No auditing	No auditing	No auditing
§ Credential Validation	Success	Success and Failure	Success	Success and Failure
§ Kerberos Service Ticket Operations	No auditing	No auditing	No auditing	No auditing
§ Other Account Logon Events **Note** No events map to this category.	No auditing	No auditing	No auditing	No auditing

Note § - Denotes Group Policy settings that are new in Windows Vista or Windows Server 2008.

Modifying Audit Policy Settings

To modify the audit policy subcategories and settings configured by the GPOs for this security guide requires you to use Auditpol.exe to modify the configuration of one computer in your environment, and then generate a file that contains the audit policy settings for your environment. The computer GPOs for this security guide can then apply the modified audit policy to computers in your environment.

To modify your audit policy configuration

1. Log on as a domain administrator to a computer running Windows Vista or Windows Server 2008 that is joined to the domain using Active Directory in which you will create the GPOs.
2. On the desktop, click the **Start** button, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog appears, verify the operation is what you requested, and click **Continue**.
4. Clear the current audit policy settings by typing the following line at the command prompt, and then press ENTER:

   ```
   auditpol /clear
   ```

5. Use the Auditpol.exe command-line tool to configure the custom audit policy settings that you want. For example, type the following lines at the command prompt. Press ENTER after each line.

   ```
   auditpol /set /subcategory:"user account management"
   /success:enable /failure:enable
   auditpol /set /subcategory:"logon" /success:enable
   /failure:enable
   auditpol /set /subcategory:"IPSEC Main Mode" /failure:enable
   ```

   Note To see all possible categories and subcategories, type the following line at the command prompt, and then press ENTER:

   ```
   auditpol /list /subcategory:*
   ```

   Type the following line at the command prompt, and then press ENTER:

   ```
   auditpol /backup /file:EC-AuditPolicy.txt (or SSLF-
   AuditPolicy.txt)
   ```

6. Copy the new EC-AuditPolicy-MS.txt and EC-WSSGAuditPolicy-DC.txt (or SSLF-AuditPolicy-MS.txt and SSLF-AuditPolicy-DC.txt) files to the NETLOGON share of one of the domain controllers in your environment, and overwrite the existing version of the files.

   The computer GPOs included with this guide will use the new EC-AuditPolicy-MS.txt and EC-WSSGAuditPolicy-DC.txt files (or SSLF-AuditPolicy-MS.txt and SSLF-AuditPolicy-DC.txt files) to modify and configure the audit policy settings on your computers.

Removing the Audit Policy Configuration

As previously discussed, the solution implemented by the GPOs included with this guide for configuring the Audit policy subcategories creates the WSSGAudit scheduled task on all computers in your environment. If you remove the GPOs that accompany this security guide from your environment, you also might want to delete the scheduled task. The scheduled task should not affect the performance of computers running Windows Server 2008, even if you remove the GPOs included with this guide from the computers in your environment.

To delete the WSSGAudit scheduled task from the computers in your environment

1. Depending on your environment type, delete the following six files from the NETLOGON share of one of the domain controllers in your environment:

   For the EC environment:

   - EC-WSSGAuditPolicy-MS.cmd
   - EC-WSSGApplyAuditPolicy-MS.cmd
   - EC-WSSGAuditPolicy-MS.txt
   - EC-WSSGAuditPolicy-DC.cmd
   - EC-WSSGApplyAuditPolicy-DC.cmd
   - EC-WSSGAuditPolicy-DC.txt

   For the SSLF environment:

   - SSLF-WSSGAuditPolicy-MS.cmd
   - SSLF-WSSGApplyAuditPolicy-MS.cmd
   - SSLF-WSSGAuditPolicy-MS.txt
   - SSLF-WSSGAuditPolicy-DC.cmd
   - SSLF-WSSGApplyAuditPolicy-DC.cmd
   - SSLF-WSSGAuditPolicy-DC.txt
2. Create an empty text file, name it DeleteWSSGAudit.txt, and copy it to the NETLOGON share of one of the domain controllers in your environment. The text file will automatically replicate to all domain controllers in your environment.
3. The WSSGAudit scheduled task checks for the DeleteWSSGAudit.txt file every time it runs, and when it finds the file, the WSSGAudit scheduled task deletes itself. Since the WSSGAudit scheduled task is configured to run every hour, it should not take long before the task is deleted from all of the computers in your environment.

Common Security Configuration Assumptions

Microsoft recommends to use a new installation of the operating system to start your configuration work so that Server Manager optimally configures just the roles and features that you select. However, if you cannot perform a new installation, ensure to check the following common security configurations before you start a role-specific setup. This approach helps to minimize the possibility of settings from previous configurations interfering with the server's security settings for its new role.

The following table lists the common server security configuration best practices that Microsoft recommends to follow before configuring a server for a specific role. You can use this table as a checklist to help ensure that your server is appropriately configured and hardened against malicious attacks.

Table 2.10 Server Configuration Best Practice Assumptions

Component	Characteristics
Physical security	Store your servers in secure areas with restricted access to help limit unauthorized access and minimize the possibility of theft.
System Updates	After installing the operating system, use Windows Update to ensure that you have installed the latest security and system updates on the servers.
Roles	Use Server Manager to remove all unnecessary role services or features from the servers. This best practice helps minimize the attack surface of each server.
Applications, services and devices	Server Manager configures the necessary services and devices installed on each server for the roles they perform. However, any applications installed on the servers that no longer required can affect security. Microsoft recommends removing all unnecessary applications and services from each server.
Protocols	Remove or disable any unused protocols. By default, Windows Server 2008 installs the standard TCP/IP version 4 and 6 protocols for use with the installed network cards.
Accounts	Remove any unused user accounts. Ensure the Guest account is not enabled (it is disabled by default). Rename the default administrator account and establish a strong password for it. For additional protection, disable the default administrator account. Ensure strong password policies are enforced. Restrict remote logons for standard user accounts. Disable Null sessions (anonymous logons). Disable or remove shared administrative accounts. Restrict the local administrators group (ideally to two members). Require administrators to log on interactively (or implement a secure remote administration solution).
Files and directories	Use Windows Explorer to check the hard drives on the server for files or folders that are no longer required. If possible, reformat disks that contained sensitive legacy data. Ensure that the Everyone group has no rights to folders or shares containing sensitive data.

Component	Characteristics
Check Shares	Remove unused shares from the server. Remove permissions from the Everyone group from any server shares.
Review Firewall Rules	Review the status of Windows Firewall rules to ensure that only the required network ports are available to the network. The Windows Server 2008 Attack Surface Reference workbook that accompanies this guide documents the default Windows Firewall rules that Server Manger creates while configuring a server role. Review the dynamic port range configuration. For more information about dynamic ports that Windows Server 2008 requires, see Microsoft Knowledge Base article 929851: "The default dynamic port range for TCP/IP."

The remaining chapters in this guide assume that you have applied these best practices before you attempt to configure specific server roles.

More Information

The following resources provide additional information about Server Manager and the Security Configuration Wizard included with Windows Server 2008 on Microsoft.com:

- *Antivirus Defense-in-Depth Guide*.
- Security Configuration Wizard Concepts.
- Security Configuration Wizard for Windows Server 2008.
- Server Manager.
- *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.
- The default dynamic port range for TCP/IP.
- The New Windows Firewall in Windows Vista and Windows Server 2008.
- Windows Server 2008: Server Management.
- Windows Server 2008 Server Manager Technical Overview.
- Virus scanning recommendations for computers that are running Windows Server 2003, Windows 2000, Windows XP, or Windows Vista.

Chapter 3: Hardening Active Directory Domain Services

Organizations use Active Directory® Domain Services (AD DS) to manage domain users and resources, such as computers, printers, and applications on a network. AD DS in Windows Server® 2008 includes a number of new features that are not available in previous versions of Windows Server, and some of these features focus on deploying AD DS more securely.

The role services available for the Active Directory Domain Services role, as displayed in the following figure, include:

- **AD DS Domain Controller**. This role service installs by default with the AD DS role. It enables a server to store directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
- **Identity Management for UNIX**. This role service integrates computers running Windows® in an existing UNIX environment. You can install the following optional sub-elements of this role service:
    - Server for Network Information Services (NIS). This sub-element integrates Windows and NIS networks by exporting NIS domain maps to Directory Service entries. This allows an Active Directory domain controller to act as a master NIS server.
    - Password Synchronization. This sub-element ensures that when a password changes in one environment (UNIX or Windows) it also changes in the other environment.

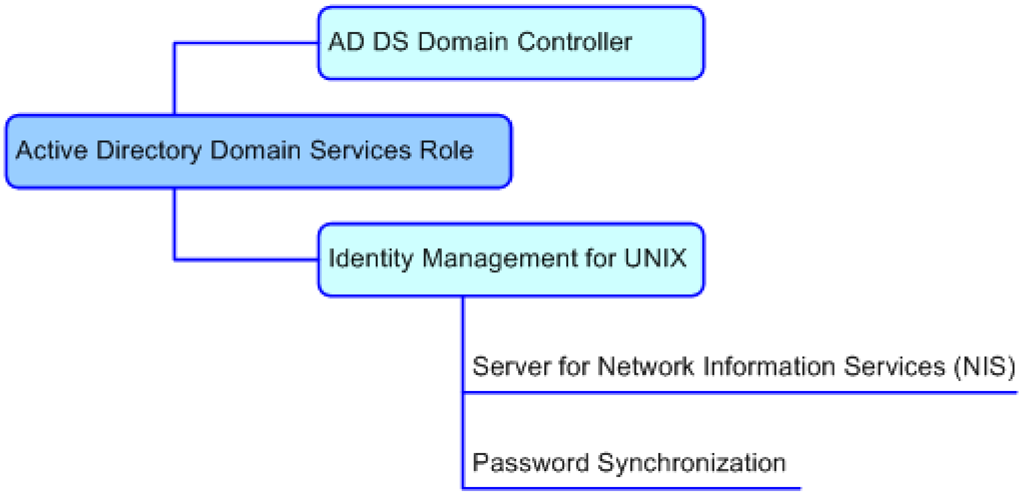

AD DS Domain Controller
Active Directory Domain Services Role
Identity Management for UNIX
Server for Network Information Services (NIS)
Password Synchronization

Figure 3.1 Role services hierarchy for the AD DS role

Active Directory Domain Controller Role Service

The Active Directory Domain Controller role service in Windows Server 2008 includes the following security-related enhancements that did not exist in previous versions of Windows Server:

- **Attribute-change auditing**. Windows Server 2008 now logs both the old and new values of an attribute when a successful change is made to that attribute. Previously, AD DS auditing only logged the name of the attribute that changed. Windows Server 2008 also includes additional subcategories for auditing AD DS. You can use these auditing-related improvements to help perform forensic analysis of security-related changes in Active Directory attributes.

  Note This enhancement affects textual attributes. For binary attributes no value is specified.

- **Fine-grained password policies**. Windows Server 2008 allows you to specify multiple password and account lockout policies within a single domain. This allows you to apply different restrictions for password and account lockout policies to different sets of users in a domain.
- **Read-only domain controller (RODC)**. Windows Server 2008 supports this new type of domain controller, which has a read-only AD DS database and only supports inbound replication for all hosted partitions and SYSVOL. These domain controllers do not maintain copies of account passwords, except for the RODC specific computer account and the RODC specific Kerberos account. This helps ensure that other sensitive data does not replicate to them. Read-only domain controllers are particularly useful in environments where you cannot guarantee physical security.

Note Although the Active Directory Domain Controller role service installs when you implement the AD DS role, the server is not considered to be a domain controller at this point. For this reason, many of the services associated with this role service are disabled. To use the Active Directory Domain Controller role service, you must promote the server to a domain controller using the Active Directory Domain Services Installation Wizard.

Attack Surface

The Active Directory Domain Controller role service is susceptible to the same security attacks as domain controllers running previous versions of Windows Server. To identify the attack surface for this role service, you need to identify the following:

- **Installed files**. The files that are installed as part of the Active Directory Domain Controller role service.
- **Running services**. The services that run as part of the Active Directory Domain Controller role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.

- **Firewall rules**. The Windows Firewall rules that the Active Directory Domain Controller role service uses.
- **Role dependencies**. The dependencies for the Active Directory Domain Controller role service.

The details of the attack surface for the Active Directory Domain Controller role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **AD DS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Active Directory Domain Controller role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Active Directory Domain Controller role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers performing the Active Directory Domain Controller role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 3.1 Configuration Checklist

	Configuration tasks
	Deploy a Server Core installation of Windows Server 2008.
	Deploy RODCs where physical security cannot be guaranteed.
	Delegate local administration of RODCs.
	Limit secure information stored on RODCs.
	Combine the DNS role service and the Domain Controller role service.
	Restrict administrator group members and administration scope.
	Prevent service administrators from bypassing password policies.
	Configure fine-grained password policies.
	Require multifactor authentication for users with elevated privileges.
	Manage service administrators in a controlled OU structure.
	Manage group membership for service administrator accounts.
	Encrypt data stored on local drives using BitLocker™ Drive Encryption.
	Backup BitLocker and TPM recovery information in Active Directory.
	Protect the computer startup key using Syskey.

Deploy a Server Core Installation of Windows Server 2008

Deploying Windows Server 2008 using the Server Core installation option reduces the attack surface of the operating system by limiting the number of required files and services. The advantage of the Server Core option is that it does not install files and services required for the graphical user interface (GUI).

When you use the Server Core installation option of Windows Server 2008 to deploy the operating system, you can only locally manage the server using command-line tools. To manage the server using GUI-based tools, you must install and run these tools on another computer with a Windows-based GUI.

You can use the following command line management tools to install, uninstall, start, and stop the AD DS role:

- To install and uninstall the AD DS role, run one of the following commands:

  ```
  dcpromo /unattend:<unattendfile>
  ```

  or

  ```
  dcpromo /unattend /option1=”value1” /option2=”value2”
  /option=…”
  ```

  Where *unattendfile* is the name of a Dcpromo.exe unattend file. You must install the AD DS role using an unattend file because the Dcpromo.exe graphical wizard is not supported.
- To start the Active Directory Domain Services service, run the following command:

  ```
  net start "Active Directory Domain Services"
  ```

- To stop the Active Directory Domain Services service, run the following command:

  ```
  net stop "Active Directory Domain Services"
  ```

See the following resources for more information about the Server Core installation option and managing AD DS from a command line:

- Managing Active Directory From the Command Line.
- Server Core.

Deploy RODCs Where Physical Security Cannot Be Guaranteed

Because of their importance, Microsoft recommends to always store domain controllers in physically secure locations that are accessible only to qualified administrative staff. If your organization must store domain controllers in unsecured locations, such as branch offices, you can use read-only domain controllers (RODCs) in these situations.

RODCs do not maintain copies of all account passwords locally, except for the RODC specific computer account and the RODC-specific Kerberos account. You can configure which account passwords are stored on an individual RODC by using the RODC-specific Password Replication Policy. Typically, most RODCs will cache a reduced set of account passwords locally, which result from the subset of those that are enabled for replication to a RODC and are accessed directly on that RODC. You can help ensure that other sensitive data does not replicate to them by using the RODC Filtered Attribute Set.

RODCs do not allow externally initiated changes to be made to the AD DS database for the following reasons:

- The AD DS database on the RODC is read-only.

- Only inbound replication is supported for all hosted partitions and the SYSVOL.

In this way, you can locate conventional domain controllers in secure data centers, and then establish a network communications path to the RODCs. However, it is also always important to bear in mind that any computer stored in a physically unsecured location represents a security risk to an organization.

Note Although RODCs do not require the same security measures as writable domain controllers, implementing as many of the same security recommendations as you do for writable domain controllers will ensure the highest possible security.

Delegate Local Administration of RODCs

The Administrator Role Separation feature for an RODC allows any domain user or security group to be delegated as the local administrator of an RODC without granting that user or group any rights for the domain or other domain controllers. Accordingly, a delegated administrator can log on to a RODC to perform maintenance work on the server, such as upgrading a driver.

However, the delegated administrator would not be able to log on to any other domain controller or perform any other administrative tasks in the domain. In this way, you can delegate a security group that comprises branch office users, rather than members of the Domain Admins group, the ability to effectively manage the RODC in the branch office without compromising the security of the rest of the domain.

Limit Secure Information Stored on RODCs

Some applications that use AD DS as a data store may have credential-like data or attributes, such as passwords, credentials, or encryption keys that you do not want to store on a RODC in case it is stolen or compromised. For this type of application, you can take the following steps to help prevent unnecessary exposure of such attributes:

- Add each attribute to the RODC filtered attribute set to prevent them from replicating to RODCs in the forest.
- Mark each attribute as confidential, which removes the ability to read the data for members of the Authenticated Users group (including any RODCs).

For more information about how to limit the secure information stored on RODCs, see "RODC filtered attribute set" on the RODC Features page for Windows Server 2008.

Combine the DNS Role Service and the Domain Controller Role Service

Windows Server 2008 domain controllers require a stable, properly configured DNS service. You can integrate DNS zones into AD DS, which is the more secure option, because this option supports secure updates.

For this reason, many organizations combine the Active Directory Domain Controller role service and the DNS role service on the same computer when the DNS role service is supporting Active Directory. However, Microsoft recommends to avoid combining the Active Directory Domain Controller role service with other server roles, except for the DNS role service that supports Active Directory. Running all other server roles on different servers minimizes the attack surface for the Active Directory Domain Controller role service.

Avoid Combining the Domain Controller Role Service with Other Role Services

Although it is possible to install other role services on computers with the Active Directory Domain Controller role service, Microsoft recommends to avoid this whenever possible. This is because combining roles in this way can cause undesirable situations to arise. For example, users with accounts in Active Directory Directory Services (AD DS) may have too much access to data associated with other role service or conversely, users accessing the network services provided by the other role service may have inappropriate access to information stored in AD DS. Installing certain role services with the Active Directory Domain Controller role service can be particularly risky, such as the Routing and Remote Access role service or those available with Active Directory Certificate Services.

Restrict Administrator Group Members and Administration Scope

Microsoft recommends limiting administrator access to the writable domain controllers in your organization to a restricted group of dedicated administrators, and separating administrative responsibilities to ensure that no one individual has too much control over Active Directory in your environment. Typically this involves subdividing administrative tasks and roles, and creating groups that correspond to those tasks and roles. For RODCs, you can implement Administrator Role Separation (ARS), as shown on the RODC Administration page on TechNet.

Other administrative tasks that you can perform to increase the security of the Active Directory Domain Controller role service include the following:

- Disable or delete unused user and computer accounts.
- Disable the Guest account.
- Rename the default administrator account, assign it a highly complex password, and then disable it by using a Group Policy object.
- Enforce password complexity rules.
- Disallow shared accounts.

Prevent Service Administrators from Bypassing Password Policies

A user with elevated privileges who is able to create user objects or has the modify permission on the **useraccountcontrol** attribute can bypass password policies. For example, by default a member of the Domain Admins group can restore a password that has expired or can enable or disable the **password not required** extended right for user objects.

You can help prevent this default behavior by configuring the following extended rights in Active Directory:

- **Enable-Per-User-Reversibly-Encrypted-Password**. This extended control access right allows users to enable or disable the **reversible encrypted password** extended right for user and computer objects.
- **Unexpire-Password**. This extended control access right allows a user to restore an expired password for a user object.

- **Update-Password-Not-Required-Bit**. This extended control access right allows a user to enable or disable the **password not required** extended right for user objects.

For more information about configuring extended rights in Active Directory, see the following resources:

- Appendix D: Active Directory Extended Rights.
- Best Practices for Delegating Active Directory.

Configure Fine-Grained Password Policies

Windows Server 2008 allows you to specify multiple password policies within a single domain, which are also known as fine-grained password policies. This allows you to maintain a minimum level of password security throughout the domain, but also require more restrictive password policies for specific user and computer groups.

You can use fine-grained password policies to apply different restrictions for password and account lockout policies to different sets of users in a domain. For example, you can apply more strict settings to privileged accounts and less strict settings to the accounts of other users. In other cases, you might want to apply a special password policy for accounts with passwords that synchronize with other data sources. Examples of this could include accounts used by UNIX computers that require less restrictive password policies.

Specifically, configure more restrictive password policies for the following users:

- Members of the Enterprise Admins security group.
- Members of the Domain Admins security group.
- Members of the Schema Admins security group.
- Members of the DHCP Admins security group.
- Members of the DNS Admins security group.
- Members of the Server Operators security group.
- Members of the Backup and Restore Operators security group.
- Members of the Administrators security group.
- Members of the Policy Administrators security group.
- Members of the Certificate Administrators security group.
- Members of the Cryptographic Administrators security group.
- Members of the Print Operators security group.
- Members of security groups with delegated administration permissions for AD DS, such as help desk personnel.
- Members of security groups with delegated administration permissions for applications that run on server computers, such as administrators of Microsoft Exchange Server or Microsoft SQL Server®.

Fine-grained password policies apply only to user objects, or **inetOrgPerson** objects if they are used instead of user objects, and global security groups. By default, only members of the Domain Admins group can create, configure and view fine-grained password policies. You can delegate the ability to create, configure, and view these policies to other users, but the domain functional level must be Windows Server 2008. However, Microsoft recommends that only members of the Domain Admins security group be able to create or configure fine-grained password policies.

You can delegate the ability to view fine-grained password policies to users who require such delegation of administration, such as support or help desk staff. To grant these users the ability to view fine-grained password policies do the following:

1. Create a security group that contains the users who need to view the fine-grained password policies.
2. Grant the security group created in Step 1 read access to the Password Settings Container (PSC).

   The PSC is created by default under the System container in the domain. You can view it by using the Active Directory Users and Computers snap-in with Advanced features enabled. The PSC stores the Password Settings objects (PSOs) for the domain.

There may be instances in which you want to delegate which fine-grained password policy is applied to a group of users, but not actually delegate the creation of the fine-grained password policies. To achieve this, Microsoft recommends to do the following:

1. Create a fine-grained password policy object with a very restrictive setting.
2. Link the Domain Users security group to the fine-grained password policy object created in Step 1.
3. For all other fine-grained password policy objects that you create, do the following:
   a. Create a fine-grained password policy object.
   b. Create a global security group.
   c. Link the global security group created in Step b to the fine-grained password policy object created in Step a.
   d. Delegate the administration of the global security group membership to users who will manage the users in the group, which subsequently delegates which fine-grained password policy is applied to the users who are members of the global security group.

You cannot apply a fine-grained password policy to an organizational unit (OU) directly. To apply a fine-grained password policy to the users in an OU, you can use a shadow group.

A shadow group is a global security group that is logically mapped to an OU to enforce a fine-grained password policy. You add users of the OU as members of the newly created shadow group, and then link the shadow group to the fine-grained password policy. You also can create additional shadow groups for other OUs. If you move a user from one OU to another, you must update the membership of the corresponding shadow groups.

Fine-grained password policies do not interfere with custom password filters that you might use in the same domain. Organizations that have deployed custom password filters to domain controllers running Windows 2000 or Windows Server 2003 can continue to use those password filters to enforce additional password restrictions.

For more information about fine-grained password policies, see AD DS: Fine-Grained Password Policies.

Require Multifactor Authentication for Users with Elevated Privileges

Human authentication factors are generally classified into the following cases:

- The user knows specific information, such as a password, pass phrase, or personal identification number (PIN).
- The user has a specific device, such as a smart card, security token, software token, phone, or cell phone.
- The user provides a human attribute through an action, such as a fingerprint or retinal pattern, DNA sequence, signature or voice recognition, unique bio-electric signals, or another biometric identifier.

Often organizations use a combination of these methods. For example, a debit card and a PIN, which is also known as *two-factor authentication*. You can use multifactor authentication to enhance the level of authentication in your organization, compared to only requiring users to provide a password. Multifactor authentication typically includes a physical device, such as a smart card reader, USB security token, or fingerprint reader. Selecting physical devices for multifactor authentication is based on nonsecurity related requirements.

For example, your organization could require smart cards for users that include picture identification, as you can print a picture and a name on the smart card. However, a smart card requires a reader, which may introduce additional costs. A USB token can include flash memory for storing documents and files, and users can plug a USB token into existing USB ports on their computers.

This form of security is recommended for accounts with elevated privileges. Specifically, Microsoft recommends requiring multifactor authentication for the following users:

- Members of the Enterprise Admins security group.
- Members of the Domain Admins security group.
- Members of the Schema Admins security group.
- Members of the DHCP Admins security group.
- Members of the DNS Admins security group.
- Members of the Server Operators security group.
- Members of the Backup and Restore Operators security group.
- Members of the Administrators security group.
- Members of the Policy Administrators security group.
- Members of the Certificate Administrators security group.
- Members of the Cryptographic Administrators security group.
- Members of the Print Operators security group.
- Members of security groups with delegated administration permissions for AD DS, such as help desk personnel.
- Members of security groups with delegated administration permissions for applications that run on server computers, such as administrators of Exchange Server or SQL Server.

Note If possible, use multifactor authentication throughout the organization to ensure that the strongest possible passwords are required for user accounts. Using multifactor authentication causes the system to automatically generate cryptographically strong random passwords for accounts.

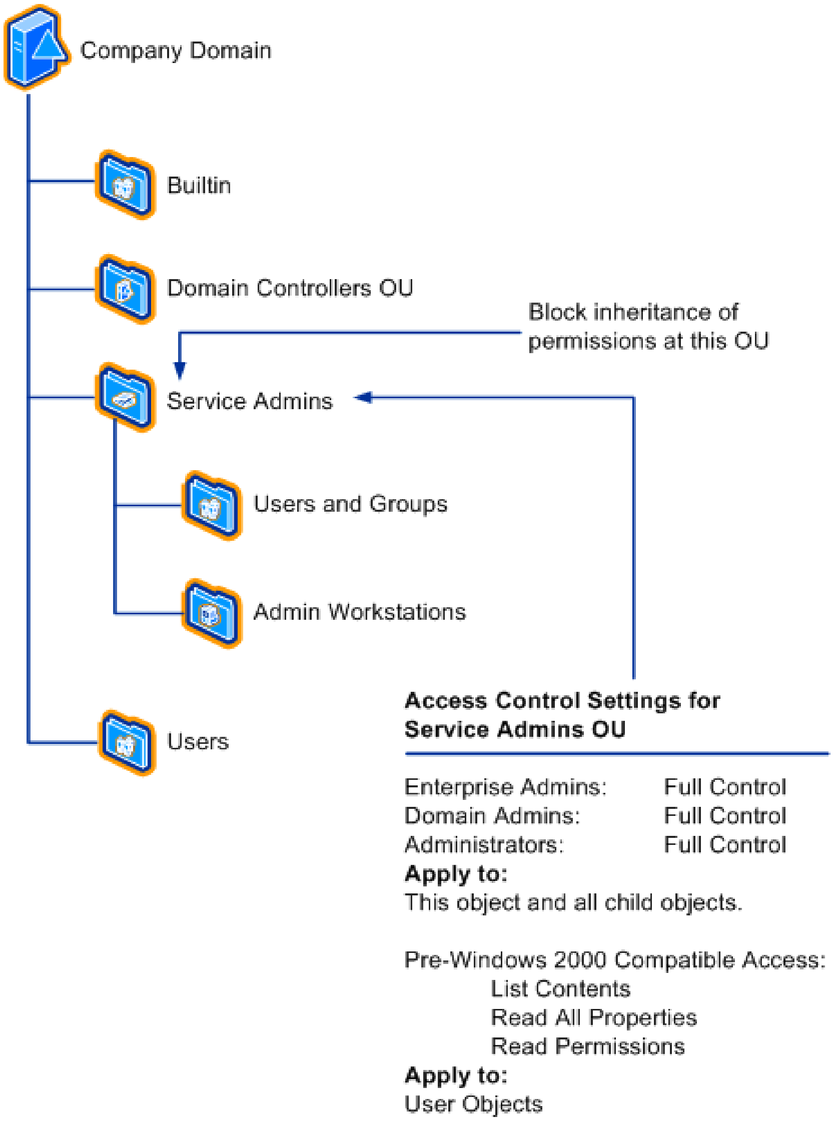
Manage Service Administrators in a Controlled OU Structure

Service administrators are responsible for the delivery of the directory service, directory-wide settings, installation and maintenance of software, and application of operating system service packs and fixes on domain controllers. To perform these functions, service administrators must have physical access to domain controllers.

To help protect highly privileged service administrator accounts, allow only service administrators to manage service administrator accounts. Because such accounts have elevated privileges, data administrators should not be given the authority to modify these accounts. Doing so allows data administrators to elevate their privileges. Service administrator accounts should be accessed and managed in a highly-controlled subtree in each domain.

To provide a more controlled environment that facilitates the management of service administrator accounts and workstations, create a controlled OU structure to manage service administrator accounts in Active Directory, as shown in the following figure. A member of the Domain Admins group should create a controlled OU structure for each domain, and configure each of the OUs with the recommended security settings.

By creating an OU structure that contains all service administrator accounts and the administrative workstations that they use, you can apply controlled security and policy settings to the structure to maximize protection of the accounts and computers. The following figure displays an example of a controlled administrative OU structure and its access control settings.



Access Control Settings for Service Admins OU

Enterprise Admins:	Full Control
Domain Admins:	Full Control
Administrators:	Full Control

Apply to:
This object and all child objects.

Pre-Windows 2000 Compatible Access:
List Contents
Read All Properties
Read Permissions

Apply to:
User Objects

Figure 3.2 Sample OU structure for managing service administrator accounts

To create a controlled OU structure, perform the following steps:

1. Create the OU structure.
2. Set the access control lists (ACLs) on the controlled OUs.
3. Add service administrator groups to the controlled OU structure.
4. Add service administrator user accounts to the controlled OU structure.
5. Add the computer accounts for the administrator workstations to the controlled OU structure.

Step 1: Create the OU Structure

Create a high-level OU to hold the groups and user accounts that constitute your service administrators and their workstations. Within this OU, create another OU to hold administrative user and group accounts, and another OU to hold administrative workstations.

The previous figure depicts a recommended OU hierarchy for a controlled subtree to manage service administrator accounts and workstations. It consists of a controlled OU structure rooted at the Service Admins OU that contains two additional OUs: the Users and Groups OU, to hold the administrative user and group accounts, and the Administrative Workstations OU, to hold the computer accounts of the workstations that the service administrators use.

Step 2: Set the ACLs on the Controlled OUs

Depending on the rest of our OU structure, users with delegated administration permissions might inadvertently have permissions to administer the users in the controlled OUs. You need to change the ACLs on the controlled OUs so that only specific service administrators can administer the membership of service administrator users, groups, and workstations. This prevents the controlled OUs from inadvertently inheriting permission configuration changes in GPO settings that are higher in the OU structure.

To limit access to the controlled OUs, do the following:

- Block inheritance of permissions on the Service Admins OU so that changes made to GPO settings higher in the OU structure cannot be inherited in the lower structure to alter locked-down settings.
- Set the ACL on the Service Administrators OU, as indicated in the following table.

Table 3.2 ACL Settings for the Service Administrators OU

Type	Name	Access	Applies to
Allow	Enterprise Admins	Full Control	This object and all child objects.
Allow	Domain Admins	Full Control	This object and all child objects.
Allow	Administrators	Full Control	This object and all child objects.
Allow	Pre-Windows 2000 Compatible Access	List Contents Read All Properties Read Permissions	User objects.

Step 3: Add Service Administrator Groups to the Controlled OU Structure

Move the following service administrator groups from their current location in the directory into the Users and Groups OU in your controlled OU structure:

- Domain Admins
- Enterprise Admins (if this is the root domain of the forest)
- Schema Admins (if this is the root domain of the forest)

For complete protection of service administrator groups, it would be ideal to move the built-in groups, which include Administrators, Server Operators, Account Operators, and Backup Operators to the controlled OU structure. However, you cannot move built-in groups from their default container. Step 6 explains how to protect the accounts of members who belong to these groups.

Step 4: Add Service Administrator User Accounts to the Controlled OU Structure

Move all administrative user accounts that are members of any of the service administrator groups listed in step 3 from their current locations in the directory into the Users and Groups OU in your controlled OU structure. Be certain to move the built-in domain Administrator account as part of this process.

Microsoft recommends providing each service administrator with two accounts: one for administrative duties, and one for their normal user access. Place the administrative user accounts in the Users and Groups OU in your controlled OU structure. If these accounts already exist elsewhere in the directory, move them into the OU structure as part of this step. Do not place the regular user accounts for these administrators in this controlled OU structure.

Step 5: Add the Computer Accounts for the Administrator Workstations to the Controlled OU Structure

Designate administrator computers as administrative workstations. Move the computer accounts for these workstations into the Administrative Workstations OU in your controlled OU structure.

Important Do not move any domain controller accounts out of the default Domain Controllers OU, even if some administrators log on to them to perform administrative tasks. Moving domain controller accounts will disrupt the consistent application of domain controller policies to all domains in your environment.

Manage Group Membership for Service Administrator Accounts

To enhance security, limit the membership in each of the service administrator groups to the absolute minimum that your organizational logistics allow, while preserving your ability to manage Active Directory service functions. This reduces the number of possible administrative accounts an attacker can possibly compromise. The following sections explain some recommended practices for managing the membership of the service administrator groups.

Assign Trustworthy Personnel

Assign only trustworthy personnel with service administrator control of the configuration and the directory service. This responsibility should only be entrusted to reliable, trusted users who have demonstrated responsible ownership, and who fully understand how to maintain the directory. These administrators should be completely familiar with your organization’s security and operations policies, and they should have demonstrated their willingness to enforce them.

Restrict Service Group Membership to Users in the Forest

Microsoft recommends not including users or groups from another forest as members of service administrator groups, unless you completely trust the service administrators of the other forest. Because service administrators in the other forest have full control on the user accounts in that forest, they can easily impersonate or authenticate to your forest using the credentials of one of those users. Furthermore, trusting the remote domain (or forest) in this way also places your trust in the remote domain's security measures, which is something that you cannot control.

Note If you determine that you need to establish a trust with another forest, implement security identifier (SID) filtering between the forests. SID filtering is enabled on external trusts by default, but is not enabled on forest trusts. This prevents the administrator of one forest (Forest A) from gaining elevated permissions in the other forest (Forest B) by injecting the SID of the Domain Admins security group in Forest A into the **sidhistory** attribute of his account in Forest B.

If it is necessary for an administrator from another forest to act as a service administrator in your domain, create an account in your domain that the administrator can use to perform administrative tasks. Creating such an account eliminates your dependence on the security measures of the other forest.

Limit the Schema Admins Group to Temporary Members

The Schema Admins group is a special group in the forest root domain that provides administrative access to the Active Directory schema. Members of this group have the necessary user rights to make changes to the schema. In general, because schema changes are only made rarely, it is not necessary for a schema administrator to be available at all times. This account is only needed when a schema update must be processed or if a change must be made to the configuration of the schema operations master role holder.

To minimize the possibility of an Active Directory attack through a schema administrator account, Microsoft recommends keeping the membership of the Schema Admins group empty. Add a trusted user to the group only when an administrative task must be performed on the schema. Remove the member after the task is completed.

Limit Administrator Rights to Those Rights That Are Actually Required

Active Directory contains a built-in group named Backup Operators. Members of this group are considered service administrators, because the group’s members have the privilege to log on locally and restore files, including the system files, on domain controllers. Microsoft recommends to limit membership in the Backup Operators group in Active Directory to only those individuals who backup and restore domain controllers.

All member servers also contain a built-in group called Backup Operators that is local to each server. Microsoft recommends to make individuals who are responsible for backing up applications, such as SQL Server on a member server, members of the local Backup Operators group on that server, instead of making them members of the Backup Operators group in Active Directory. Limit the membership of the Backup Operators Group in Active Directory to those individuals who backup and restore domain controllers.

On a dedicated domain controller, you can reduce the number of members in the Backup Operators group. When a domain controller is used to run other applications, as it might be in a branch office, individuals who are responsible for backing up applications on the domain controller must also be trusted as service administrators. This is because they require privileges necessary to restore files, including system files, on domain controllers.

Avoid using the Account Operators group to strictly delegate "data administration" tasks, such as account management. Because the default directory permissions give this group the ability to modify the membership of other service administrator groups, such as Server Operators, members of the Account Operators group can elevate their privileges to become service administrators. By default, there are no members in the Account Operators group, and its membership should be left empty.

Microsoft recommends creating custom security groups and assigning these groups necessary rights and permissions instead of using built-in groups. This is because the existing built-in groups are typically assigned more rights and permissions than necessary to perform a specified role. Creating custom groups allows you to assign only the rights and permissions that are necessary for an individual to perform a specific role in your organization. For example, you could create a new security group called Help Desk Staff and then assign this security group only the necessary rights and permissions that members who belong to it require to perform their role.

Encrypt Data on Local Drives Using BitLocker Drive Encryption

BitLocker Drive Encryption is a data protection feature available in the Windows Vista® Enterprise and Windows Vista® Ultimate operating systems for client computers, and in Windows Server 2008. BitLocker provides enhanced protection against data theft or exposure on computers that are lost or stolen, and more secure data deletion when BitLocker-protected computers are decommissioned.

Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software attack tool against it or by transferring the computer’s hard disk to a different computer. BitLocker helps mitigate unauthorized data access on lost or stolen computers by combining two major data-protection procedures:

- Encrypting the entire Windows operating system volume and data volumes on the hard disk. BitLocker encrypts all user files and system files in the operating system volume, including the swap and hibernation files, and can also encrypt data volumes.
- Checking the integrity of early boot components and boot configuration data. On computers that have Trusted Platform Module (TPM) version 1.2, BitLocker leverages the enhanced security capabilities of the TPM to help ensure that your data is accessible only if the computer’s boot components appear unaltered and the encrypted disk is located in the original computer.

Because a writable domain controller contains all domain account passwords, X.509 certificates, and other security-related information, encrypting the volumes by using BitLocker provides additional protection in the event that a domain controller, or a domain controller hard drive, is stolen. RODCs contain a subset of this information, but Microsoft still recommends encrypting the volumes by using BitLocker. For more information about configuring BitLocker for Windows Server 2008, see the *BitLocker Drive Encryption Step-by-Step Guide*.

Note Secure the BitLocker volume master keys by using TPM and a startup key or TPM and a PIN on domain controllers. Do not use TPM only as a method for securing the volume master keys for domain controllers.

For more information about best practices for using BitLocker, see the following resources:

- BitLocker Drive Encryption.
- IT Showcase: Optimizing Client Security by Using Windows Vista.

Backup BitLocker and TPM Recovery Information in Active Directory

During installation, a recovery password is created for each BitLocker-enabled volume. If you also use TPM, you also must specify the TPM owner password. You can store the recovery information required for these technologies in AD DS.

Backing up recovery passwords for a BitLocker-protected disk volume allows administrators to recover the volume if it is locked. This ensures that authorized users always can access encrypted data belonging to the enterprise.

Note This method for backing up recovery passwords assumes you have more than one domain controller in your organization. If you have only one domain controller, then also copy the recovery passwords to removable media.

Backing up the TPM owner information for a computer allows administrators to locally and remotely configure the TPM security hardware on that computer. As an example, an administrator might want to reset the TPM to factory defaults when decommissioning or repurposing computers.

For more information about how to configure AD DS to back up BitLocker and TPM recovery information, see *BitLocker Drive Encryption Configuration Guide*.

Protect the Computer Startup Key Using Syskey

In secure datacenter environments, generally only authorized personnel can restart domain controllers. However, in an environment where you cannot strictly enforce these recommendations, such as in branch offices, there is increased potential for an unauthorized person to restart a domain controller.

An unplanned or unexpected restart of a domain controller can indicate that an attacker has started the domain controller with an alternate operating system and compromised its security. On the other hand, the restart might simply be due to a loss of power or to scheduled maintenance on the domain controller. The following sections include SYSKEY methods, dependencies, and considerations that you can use to determine how best to use SYSKEY in your environment.

Determining if SYSKEY Is Appropriate for Your Environment

The system key (SYSKEY) in Windows operating systems protects security information, including passwords in the Active Directory database and other Local Security Authority (LSA) secrets, against offline attacks by encrypting their storage on the domain controller. SYSKEY can either be derived from a secret password that you specify, or you can store it on removable media, such as a floppy disk or USB drive.

Note SYSKEY protects only the security information in Active Directory or other LSA secrets. BitLocker protects all data stored on BitLocker-encrypted volumes. In instances where encrypting the entire volume is inappropriate, use SYSKEY to protect Active Directory information and LSA secrets.

When starting a domain controller protected by this method, you must either supply the password or the removable media containing SYSKEY to successfully restart the computer. You can use the system key utility (Syskey.exe), which installs on the domain controller with Windows Server 2008, to select which of these methods you want to use to start the computer.

Implementing SYSKEY provides the following security advantages:

- Point-in-time control of the domain controller restart, which evaluates the reason for the domain controller restart, and determines if security has been compromised.
- Protection for passwords stored in the directory database against offline attacks if the domain controller or a disk is stolen.

There are certain logistic operational issues with SYSKEY. The first of these is the management of SYSKEY passwords or removable media. For example, requiring a branch manager or local administrative staff to come to the office at 3 A.M. to enter passwords or insert removable media might be problematic.

To help mitigate this problem, you can allow centralized IT operations personnel to provide the SYSKEY password remotely, which requires additional hardware to support remote management. These remote methods allow the IT operations personnel to type the password or mount virtual images of the floppy containing the SYSKEY.

The other potential logistical problem is that losing the SYSKEY password or removable media leaves the domain controller in a state in which no one can restart it. There is no way to recover a domain controller if the SYSKEY password or floppy disk is lost. In this situation, it would be necessary to rebuild the domain controller.

Each method has advantages and potential difficulties. If you choose to add SYSKEY protection to your domain controllers, first evaluate your security environment to determine which method will work best for your organization.

Providing SYSKEY Passwords for Domain Controller Restarts

The advantage of providing SYSKEY passwords is that they do not require physical media that can be lost. Trusted personnel must type a password at a console connected to the domain controller in the event that it needs to be restarted. The password should be known to only a small group of trusted administrators, preferably only members of the Domain Admins group. The disadvantages of using a password to secure SYSKEY are that trusted personnel are required to memorize another password and they must be on site to use the password.

To support branch offices, you may need to provide the SYSKEY password remotely through central IT trusted personnel. However, this requires using additional hardware to support remote management.

Because attackers can compromise passwords, Microsoft recommends to increase the security of passwords for SYSKEY restarts by doing the following:

- Use strong passwords.
- Store the passwords in a secure place, such as a bank safety deposit box.
- Require SYSKEY passwords to be periodically changed.

Providing SYSKEY on Removable Media for Domain Controller Restarts

The advantage of providing SYSKEY on removable media is that it does not require trusted personnel to memorize a password. However, implementing SYSKEY with removable media does introduce the risk of lost or damaged physical media. Furthermore, trusted personnel are required to insert the removable media during domain controller restarts. Again, only trusted personnel, preferably members of the Domain Admins group, should have access to the SYSKEY removable media.

To support branch offices, you may need to install third-party hardware devices to support remote management, so that floppy disk images can be remotely transferred to the domain controller. Using these devices, central IT trusted personnel can transfer a copy of the SYSKEY disk image to a remote domain controller. After the domain controller restarts, IT operations personnel can delete the remote image of the SYSKEY floppy disk.

Because the removable media contains the cryptographic key for SYSKEY, you should take measures to ensure that the removable media is not stolen, lost, destroyed, or copied by an unauthorized person. Microsoft recommends the following measures to mitigate these risks:

- Copy the removable media and store the copy at an off-site location, such as in a bank safe deposit box.
- Store the working copy of the removable media in a secure place on site.
- Remove the removable media from the domain controller immediately after it restarts.

Relevant Group Policy Settings

The Domain Controller Baseline Policy (DCBP) that complements the Default Domain Controller Policy is linked to the Domain Controllers organizational unit (OU). The DCBP settings enhance overall security for domain controllers in any environment. Using only two GPOs to secure domain controllers allows the default environment to be preserved and simplifies troubleshooting.

For more information about these settings, see the Windows Server 2008 Security Baseline Settings workbook.

More Information

The following resource provides further security best practice information about how to harden servers running the Active Directory Domain Controller role service:

- Active Directory Domain Services.
- AD DS: Fine-Grained Password Policies.
- Appendix D: Active Directory Extended Rights.
- Best Practices for Delegating Active Directory.
- BitLocker Drive Encryption.
- *BitLocker Drive Encryption Configuration Guide*.
- *BitLocker Drive Encryption Step-by-Step Guide*.
- IT Showcase: Optimizing Client Security by Using Windows Vista.
- Managing Active Directory From the Command Line.
- RODC Administration.
- "RODC filtered attribute set" on the RODC Features page.
- Server Core.
- Set computer-specific synchronization properties.

Identity Management for UNIX Role Service

With the Identity Management for UNIX role service, you can authenticate credentials in Active Directory using the Network Information Services (NIS) protocol, and you can synchronize account passwords stored in Active Directory with account passwords stored in NIS servers running UNIX. The Identity Management for UNIX role service comprises the following sub-element role services:

- **Server for Network Information Services**
- **Password Synchronization**

Each of these sub-element role services are discussed in subsequent sections. For more information about the Identity Management for UNIX role service, see the "Overview of Identity Management for UNIX" in the Help and Support for Windows Server 2008.

Server for Network Information Services

The Server for NIS sub-element integrates Microsoft Windows® and NIS networks by providing a Windows–based AD DS domain controller with the ability to act as a master NIS server for one or more NIS domains.

Server for NIS stores both standard and nonstandard NIS map data in AD DS, and creates a single name space for the Windows and NIS domains that a Windows administrator can manage using a single set of tools. The administrator can easily create, modify, and delete user accounts for Windows and NIS-enabled UNIX domains at the same time. A user who has accounts in both Windows and UNIX environments can be managed by AD DS with all of the attributes necessary for the respective domain and name space.

Server for NIS is typically used in conjunction with Server for Network File System (NFS). NFS provides shared network file services for NFS clients, which are typically found on computers running UNIX. For more information about the Network Information Services role service, see the "Server for NIS" section in the Help and Support for Windows Server 2008.

Attack Surface

The Server for Network Information Services (NIS) role service is susceptible to the same security attacks as any NIS server. To identify the attack surface for this role service, you need to identify the following:

- **Installed files**. The files that are installed as part of the Server for NIS role service.
- **Running services**. The services that run as part of the Server for NIS role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the Server for NIS role service uses.
- **Role dependencies**. These are dependencies for the Server for NIS role service.

The details of the attack surface for the Server for NIS role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this server role, on the **AD DS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Server for NIS role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Server for Network Information Services role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks to harden servers that perform the Server for NIS role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 3.3 Configuration Checklist

	Configuration tasks
	Configure the computer to run Server for NIS in master mode.
	Require users to change their Windows passwords.

Note The Server for Network Information Services role service is not available on Server Core installations of Windows Server 2008.

Configure the Computer to Run Server for NIS in Master Mode

To operate Network Information Services (NIS), a computer can run these services in *master mode* or *subordinate mode*. The primary difference between the two modes is that both subordinate and master servers can read map data, while only the master server can update maps. In addition, the master NIS server provides periodic updates of the maps to subordinate servers.

Configure one of the computers running Server for NIS to be the master NIS server. This ensures that the Windows-based master NIS server will receive updates from the other NIS servers running in subordinate mode. Because the data is stored in Active Directory, the security for the data is stronger than is typically available by storing it in a file on UNIX.

For more information about master mode, subordinate mode, and the interaction between computers running these modes, see "Master and subordinate server modes" in the Help and Support for Windows Server 2008.

Require Users to Change Their Windows Passwords

Typically, users running UNIX or LINUX operating systems change their NIS passwords by running the **yppasswd** command. This command is used to update the user's password in NIS. The **yppasswd** command sends the old password to the NIS server in plaintext. For this reason, this command might expose the user's Windows password.

Instead of using this command, users should change their NIS password by changing their Windows passwords. The server running Network Information Services will then synchronize the password change with the subordinate NIS servers.

Relevant Group Policy Settings

There are no Group Policy settings available for the Server for NIS role service.

More Information

For more security best practice information about how to harden server computers running the Server for NIS role service, see "Server for NIS" in the Help and Support for Windows Server 2008.

Password Synchronization

The Password Synchronization role service helps you integrate Windows and UNIX networks by simplifying the process of maintaining secure passwords in both environments. This reduces the effort required to maintain separate passwords for Windows and UNIX accounts and change the password in both systems. With the Password Synchronization role service, whenever users change their passwords on a Windows-based computer in a domain, the passwords are automatically changed on every UNIX host on which the users have an account. You also can configure the Password Synchronization role service to change Windows-based user passwords automatically whenever users change their UNIX passwords.

For more information about the Password Synchronization role service, see "Password Synchronization" in the Help and Support for Windows Server 2008.

Attack Surface

The Password Synchronization role service is susceptible to the same security attacks as any AD DS domain controller. To identify the attack surface for this role service, you need to identify the following:

- **Installed files**. The files that are installed as part of the Password Synchronization role service.
- **Running services**. The services that run as part of the Password Synchronization role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the Password Synchronization role service uses.
- **Role dependencies**. The dependencies for the Password Synchronization role service.

The details of the attack surface for the Password Synchronization role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this server role, on the **AD DS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Password Synchronization role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Password Synchronization role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers that perform the Password Synchronization role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 3.4 Configuration Checklist

	Configuration tasks
	Ensure the Windows and UNIX password policies are consistent.
	Specify a computer-specific password encryption key.
	Explicitly list users allowed or blocked from password synchronization.
	Block password synchronization of disabled UNIX user accounts.
	Avoid synchronizing passwords for user accounts with elevated privileges.
	Do not use the default port number and encryption key.

	Configuration tasks
	Secure the sso.conf file.
	Ensure that the directory identified by TEMP_FILE_PATH on the UNIX host is properly protected.
	Ensure that log files are appropriately protected on the UNIX host.

Note The Password Synchronization role service is not available on Server Core installations of Windows Server 2008.

Ensure the Windows and UNIX Password Policies Are Consistent

If you are providing only one-way password synchronization, ensure that the password policy on the computer from which passwords will be synchronized is at least as restrictive as the policy on the computer to which it will synchronize passwords. For example, if you configure Windows-to-UNIX synchronization, the Windows password policy must be at least as restrictive as the policy of the UNIX computers with which it will synchronize passwords.

If you are supporting two-way synchronization, the password policies must be equally restrictive on both systems. Failure to ensure that password policies are consistent can result in synchronization failure when a user changes a password on the less restrictive system, or the password might be changed on the more restrictive system even though it does not conform to the system's policies.

Also ensure that Windows users are aware of any special password restrictions on UNIX systems with which they will synchronize their passwords. For example, some versions of UNIX support a maximum password length of eight characters. For maximum compatibility with the default Windows password policy and these UNIX limitations, limit passwords to seven or eight characters in length unless you are sure that all of the UNIX systems in your environment can support longer passwords.

Specify a Computer-Specific Password Encryption Key

A Windows-based computer can send and receive updated passwords from a UNIX-based computer as encrypted text only. The Password Synchronization single sign-on daemon (SSOD) receives the encrypted password and decrypts it before requesting the password change on the UNIX host.

Similarly, if you configure Password Synchronization to support UNIX-to-Windows synchronization, the pluggable authentication module (PAM) encrypts the password before sending it to Password Synchronization on the Windows-based computer, which then decrypts the password before requesting the password change on the Windows-based computer.

For added security, you can specify an encryption key for use only between a specific Windows-based computer and a UNIX host. This helps ensure that only specific computers can decrypt passwords from each other. For more information, see Set computer-specific synchronization properties.

Explicitly List Users Allowed or Blocked From Password Synchronization

To provide maximum control over which users can synchronize passwords, do not use the ALL keyword with the SYNC_USERS list in the sso.conf file on the UNIX host. Instead, explicitly list each user who you want to allow or block from password synchronization.

On the Windows-based computer running Password Synchronization, create the PasswordPropAllow group, and then add the accounts of users whose passwords you want to synchronize to this group. For more information about this topic, see Controlling password synchronization for user accounts.

Block Password Synchronization of Disabled UNIX Accounts

In some versions of UNIX, changing the password of a disabled user account activates that account. Consequently, if a user has a disabled account on a UNIX computer that is configured to synchronize passwords with a Windows-based computer, the user or an administrator can activate the UNIX account by changing the user's Windows password.

To prevent this, use the PasswordPropDeny group to block synchronization for disabled UNIX accounts. Also, when you disable a UNIX account, ensure that you use the SYNC_USERS entry in the sso.conf file to block password synchronization for the account.

Avoid Synchronizing Passwords for User Accounts with Elevated Privileges

Do not synchronize passwords for members of Windows groups with elevated privileges or the owners of the UNIX superuser or root accounts, because these accounts do not have elevated permissions on the other system. For example, members of the Domain Admins group have no elevated permissions on computers running UNIX by default.

Do Not Use the Default Port Number and Encryption Key

If you use the default port number and encryption key, you make it possible for an attacker to set up an impostor UNIX host to capture passwords. To help prevent imposter UNIX hosts from capturing passwords, change the value of the port and the default password encryption key used by password synchronization.

Note Protect the port number and encryption keys that you use to synchronize passwords as carefully as the passwords themselves.

For more information about these topics, see the following sections in the Help and Support for Windows Server 2008:

- "Setting the default port."
- "Setting the password encryption key."

Secure the sso.conf File

The sso.conf file on each UNIX host contains important configuration information that an attacker could use to compromise security. Microsoft recommends setting the mode bit mask of this file to 600 to better secure it.

Ensure That the Directory Identified by TEMP_FILE_PATH on the UNIX Host is Properly Protected

The temporary files created on UNIX hosts by Password Synchronization contain information that an attacker could use to compromise system security. For this reason, ensure that any directory referenced by TEMP_FILE_PATH in the sso.conf file has read access only for the root account, and that no other users access this account.

Ensure That Log Files are Appropriately Protected On the UNIX Host

Password Synchronization uses the syslogd daemon to log messages that result from synchronization operations. The resulting logs contain such information as the names of users whose passwords are synchronized with which computers, propagation errors, and so on. Ensure that only the root account can read the log files and that no other users can access the files by granting only the root account access to the directory where the logs files are stored. Check the configuration of the syslogd daemon to determine the directory where the log files are stored.

Relevant Group Policy Settings

There are no Group Policy settings available for the Password Synchronization role service.

More Information

The following resources on Microsoft.com provide further security best practice information about how to harden server computers:

- For computers running the Active Directory Domain Controller role service, see:
  - Active Directory.
  - AD DS: Fine-Grained Password.
  - Appendix D: Active Directory.
  - Best Practices for Delegating Active Directory.
  - BitLocker Drive Encryption.
  - Configuring Active Directory.
  - IT Showcase: Optimizing Client Security by Using Windows Vista.
  - Managing Active Directory.
  - "RODC filtered attribute set" in RODC Features.
  - Secure Hardware - Overview.
  - Server Core.
  - Set computer-specific synchronization properties.
- For information about the Server for Network Information Services (NIS) role service, see:
  - "Server for NIS" in the Help and Support for Windows Server 2008.
- For information about the Password Synchronization role service, see:
  - Controlling password synchronization for user accounts.
  - "Password Synchronization" in the Help and Support for Windows Server 2008.

- Set computer-specific synchronization properties.
- "Setting the default port" in the Help and Support for Windows Server 2008.
- "Setting the password encryption key" in the Help and Support for Windows Server 2008.

Chapter 4: Hardening DHCP Services

Organizations use Dynamic Host Configuration Protocol (DHCP) servers on their networks to automatically provide client computers and other TCP/IP-based network devices with valid IP addresses. DHCP can also provide additional configuration parameters for client computers and devices called *DHCP options*, which allow them to connect to other network resources, such as DNS servers and routers.

The DHCP Server service and the DHCP Client service in Windows Server® 2008 include the following security-related enhancements that did not exist in previous versions of Windows Server:

- **DHCPv6 functionality**. In Windows Server 2008, Microsoft has introduced DHCPv6 functionality to the DHCP server. Client computers use the DHCPv6 stateless mode only to obtain network configuration parameters other than the IPv6 address. In this scenario, client computers configure an IPv6 address through a mechanism not based on DHCPv6, such as through IPv6 address autoconfiguration based on the IPv6 prefixes included in Router Advertisements, or through static configuration. In the DHCPv6 stateful mode, client computers acquire both the IPv6 address, and other network configuration parameters through DHCPv6. If IPv6 is not deployed in your environment, then DHCP provides IP configuration for IPv4 addresses only. For more information about DHCPv6, see "The DHCPv6 Protocol" article on Microsoft TechNet.
- **Network Access Protection (NAP)**. NAP is integrated with DHCP to require DHCP clients to prove their system and security health state before they can receive an IP address to gain access to your intranet. NAP is supported on DHCP for IPv4 addresses, not IPv6 addresses. For more information about NAP, see the following resources:
  - "Network Access Protection."
  - *Step-by-Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab*.

This chapter provides prescriptive guidance for hardening the DHCP Server role. The DHCP Server role has no subordinate role services.

Attack Surface

The DHCP role is susceptible to many of the same security attacks as any server computer that provides DHCP services. To determine the attack surface for this role, you need to identify the following:

- **Installed files**. The files that are installed as part of the DHCP Server role.
- **Running services**. The services that run as part of the DHCP Server role.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The firewall rules that the DHCP Server role uses.
- **Role dependencies**. The dependencies for the DHCP Server role.

The details of the DHCP Server role attack surface are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this server role, on the **DHCP** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your DHCP Server role configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the DHCP Server option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers performing the DHCP Server role. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 4.1 Configuration Checklist

	Configuration tasks
	Dedicate a computer to running the DHCP Server role.
	Deploy a Server Core installation of Windows Server 2008.
	Use DHCPv6 Functionality.
	Eliminate computers running rogue DHCP services.
	Add DHCP reservation and exclusion ranges for IP addresses.
	Use NAP to enforce computer configuration health.
	Restrict DHCP security group membership.
	Configure DNS record ownership to help prevent stale DNS records.

Dedicate a Computer to Running the DHCP Server Role

Combining server roles is not generally recommended except in specific circumstances. For example, combining the DNS and AD DS server roles could be appropriate for some organizations. However, DHCP servers are often critical to the environment. Combining server roles expands the attack surface of the server, and increases the chance of a successful denial of service (DoS) attack. For these reasons, Microsoft does not typically recommend combining the DHCP server role with another role.

However, if budgetary or other reasons dictate that your organization must combine server roles, you can combine the DHCP Server role with other infrastructure server roles. A suitable combination could include the Windows Internet Name Service (WINS) server role, although many Windows Server 2008 environments no longer require a

WINS server. Microsoft recommends to avoid combining the DHCP Server role with the following roles:

- Less restrictive server roles, such as the Web Server role or the Terminal Services Server role.
- AD DS Server role, due to the importance of minimizing the attack surface of this server role.
- AD CS Server role due to the importance of minimizing the attack surface of this server role.

Deploy a Server Core Installation of Windows Server 2008

Deploying Windows Server 2008 using the Server Core installation option reduces the attack surface of the operating system by limiting the number of required files and services. The advantage of the Server Core option is that it does not install files and services required for the graphical user interface (GUI).

When you use the Server Core installation option of Windows Server 2008 to deploy the operating system, you can only locally manage the server using command-line tools. To manage the server using GUI-based tools, you must install and run these tools on another computer with a Windows-based GUI.

You can use the following command line management tools to manage the DHCP Server role:

- To install the DHCP Server role, run the following command:

  ```
  start /w ocsetup DHCPServerCore
  ```

- To configure the DHCP Server service, run the following command:

  ```
  sc config dhcpserver start = auto
  ```

  Note A space is required between "start" and "=". Also, a space is required between "=" and "auto".
- To start the DHCP Server service, run the following command:

  ```
  net start dhcpserver
  ```

- To configure DHCP servers, DHCP scopes and DHCP scope options, run the following commands:

  ```
  netsh DHCP
  netsh DHCP server
  netsh DHCP server scope
  netsh DHCP server mscope
  ```

  For more information about managing the DHCP Server role using netsh, see Netsh commands for DHCP.
- To uninstall the DHCP Server role, run the following command:

  ```
  start /w ocsetup DHCPServerCore /uninstall
  ```

For more information about installing and managing the DHCP Server role using the Server Core installation option, see the *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.

Use DHCPv6 Functionality

IPv6 allows computers to obtain IP addresses automatically using stateless autoconfiguration. This protocol does not require a DHCP server, and it ensures IP addresses are unique by using the media access control (MAC) address of the network adapter as part of the overall address, and then sending a multicast packet to determine if any other hosts on the network segment have the same IP address.

If the DHCP server uses stateless autoconfiguration, you can still use the server to provide additional network configuration options. Although Windows Server 2008 supports stateless autoconfiguration, use the stateful mode in DHCP to provide IPv6 address allocation.

The addresses generated by a DHCPv6 server are sparsely distributed over the available address space of a subnet. Potential attackers are less likely to guess IPv6 network addresses because the DHCP Server can randomly distribute the addresses over a large address range that the 64-bit IPv6 prefix makes available.

The DHCP Server role also supports permanent and temporary addresses through DHCPv6. You can use a permanent IPv6 address for Dynamic DNS registration, so that the client computer is "known" by that address. You also can use a temporary IPv6 address to establish outgoing connections for scenarios in which the client computer requires privacy for a permanent address. Administrators can automate the IPv6 configuration of computers to use the stateless or stateful mode by using Router Advertisements.

Eliminate Computers Running Rogue DHCP Services

One of the most common forms of attack involving DHCP servers is to use rogue servers to supply addresses to client computers. In most cases, this is an easy attack to launch, because it involves simply adding an additional DHCP server to the network that services client computers.

To help prevent rogue DHCP servers, Windows Server 2008 supports server authorization in Active Directory®. In order for a Windows Server 2008–based computer that is part of a domain to issue addresses, it must first be authorized in Active Directory.

Stand-alone servers that are running a Windows Server® operating system do not have to be authorized in Active Directory to issue DHCP leases. However, if a stand-alone DHCP server determines an existing domain, the stand-alone DHCP server discontinues issuing future IP addresses.

If a DHCP server is not running a Windows Server operating system, the DHCP server in the domain cannot notify the non-Windows-based computer to discontinue issuing IP addresses. To stop a non-Windows-based computer from providing DHCP services, Microsoft recommends to prevent computers from accessing the internal network by using other mechanisms, such as physical controls over Ethernet and wireless connections.

You can use the DHCPLoc command-line tool to help identify rogue DHCP servers by obtaining a list of all DHCP servers on the local subnet. The DHCPLoc tool is available in the Windows Support Tools in the \Support\Tools folder on the product CD for Windows® XP, Windows Vista®, Windows Server® 2003, and Windows Server 2008.

For more information about the DHCPLoc utility, see the Dhcploc Overview page on TechNet.

Add DHCP Reservation and Exclusion Ranges for IP Addresses

You can help ensure that computers are assigned valid IP addresses by doing the following:

- Reserve statically configured addresses so that they are not inadvertently allocated to other IP devices.
- Configure a range of IP addresses to pre-allocate them for other devices.

Note If a reservation is configured for an IP address and the IP address falls within the range of an exclusion, the reservation will take precedence.

Use NAP to Enforce Computer Configuration Health

DHCP enforcement in Windows Server 2008 requires a computer to pass a health check performed by NAP before the computer is assigned an IPv4 configuration that provides access to your intranet. If a computer does not pass the health check, the computer is assigned an IPv4 configuration that only provides access to a quarantined network. The NAP health check verifies that the configuration of the target computer meets or exceeds the security requirements of your organization, such as having the most recent service packs or antivirus signature files.

DHCP enforcement through NAP enforces the health check policy requirements every time a DHCP client attempts to lease or renew an IP address. If the DHCP client fails the health check, it is only allowed to access the quarantined network.

The subelements of DHCP enforcement through NAP consist of a DHCP Quarantine Enforcement Server (QES) that is part of the DHCP Server service in Windows Server 2008, and a DHCP Quarantine Enforcement Client (QEC) that is part of the DHCP Client service. For more information about NAP, see Chapter 10, "Hardening Network Policy and Access Services" and the Network Access Protection page on TechNet.

Restrict DHCP Security Group Membership

You can configure security group membership to the following DHCP-related security groups in order to grant authorized users access to DHCP configuration data without having to grant them full administrative privileges:

- **DHCP Administrators**. Members of this group have the right to administer DHCP servers, but with a lower level of privilege than the Domain Admins group. Assigning DHCP administrators to the DHCP Administrators group instead of the Domain Admins group allows you to apply the principle of least privilege. You can use the Restricted Groups feature of Group Policy to ensure the membership of the DHCP Administrators group does not change. For more information about this topic, see the "Relevant Group Policy Settings" section later in this chapter.
- **DHCP Users**. Members in this group have read-only access to information through the DHCP Administration Microsoft Management Console (MMC).

Configure DNS Record Ownership to Help Prevent Stale DNS Records

You can configure a DHCP server so that it dynamically registers host (A) and pointer (PTR) resource records on behalf of DHCP clients. In this configuration, the use of secure dynamic update with DNS servers might cause stale resource records.

In some circumstances, this can cause problems. For example, if DHCP1 fails and a second backup DHCP server comes online, the second server cannot update the client name because it is not the owner of the name.

In another example, if the DHCP server performs DNS dynamic updates for legacy DHCP clients—client computers running a version of Windows® earlier than Windows® 2000—and those client computers are later upgraded to Windows 2000, Windows XP, or the Windows Server 2003 operating system, the upgraded client computer cannot take ownership of the update or update its own DNS records.

To solve this problem, a built-in security group called DnsUpdateProxy is provided. If you make all DHCP servers members of the DnsUpdateProxy group, then the records of one server can be updated by another server if the first server fails. Also, because all of the objects that are created by members of the DnsUpdateProxy group are not secured, the first server (that is not a member of the DnsUpdateProxy group) to modify the set of records associated with a DNS name becomes its owner.

Therefore, when legacy client computers are upgraded, they can take ownership of their name records at the DNS server. To eliminate these potential problems, make every DHCP server registering resource records for legacy clients a member of the DnsUpdateProxy group. You can configure the DnsUpdateProxy security group through Active Directory Users and Computers.

Relevant Group Policy Settings

The following table lists the Group Policy settings that are relevant to the DHCP Server role service. Use these Group Policy settings to enforce the appropriate security configuration for your environment. The Group Policy settings in the following table are in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Restricted Groups

Table 4.2 DHCP Server Role Service Group Policy Settings

Policy object	Description	Windows Server 2008 default
DHCP Administrators	Add user accounts as required to this group. If you add an account to this group, but do not add the same account to this policy object, the account is automatically removed and an ID 637 event is logged in the Security log if you have enabled auditing for this policy object.	Not created.

Policy object	Description	Windows Server 2008 default
DHCP Users	Add user accounts as required to this group. If you add an account to this group, but do not add the same account to this policy object, the account is automatically removed and an ID 637 event is logged in the Security log if you have enabled auditing for this policy object.	Not created.

More Information

The following resources on Microsoft.com can provide you with further security best practice information about how to harden server computers that perform the DHCP Server role:

- *Antivirus Defense-in-Depth Guide*.
- Dhcploc Overview.
- Dynamic Host Configuration Protocol (DHCP) NAP Components.
- Netsh commands for DHCP.
- Network Access Protection.
- The DHCPv6 Protocol.
- *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.
- *Services and Service Accounts Security Planning Guide*.
- *Step-by-Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab*.
- "Virus scanning recommendations for computers that are running Windows Server 2003, Windows 2000, Windows XP, or Windows Vista": Knowledge Base article 822158.

Chapter 5: Hardening DNS Services

Domain Name System (DNS) is a system for naming computers and network services that is organized into a hierarchy of domains. To make using network resources easier, name systems such as DNS provide a way to map the user-friendly name for a computer or service to other information that is associated with that name, such as an IP address. When a user types a user-friendly DNS name in an application, DNS services resolve the name to its numeric address.

DNS is a required service in domains that use Windows Server® 2008. This is because domain controllers and client computers in an Active Directory® domain use the DNS service and other services advertised through Active Directory.

The DNS Server service and DNS Client service in Windows Server 2008 include the following security-related enhancements that did not exist in previous versions of Windows Server®:

- **Background zone loading**. DNS servers hosting large DNS zones that they store using Active Directory Domain Services (AD DS) can now respond to client computer queries more quickly after a restart because the zone data now loads in the background. The DNS server can use background zone loading to begin responding to queries almost immediately after it restarts, instead of waiting until its zones are fully loaded. The DNS server can respond to queries for the nodes that it has loaded or that it can retrieve from AD DS. Background zone loading helps circumvent potential denial-of-service (DoS) attacks launched by simply rebooting DNS servers that have large zones.
- **Support for read-only domain controllers (RODCs)**. The DNS Server role in Windows Server 2008 provides support for primary read-only zones on RODCs. This makes it possible for DNS zones to replicate on RODCs located in perimeter networks, branch offices, or other unsecured environments.

This chapter provides prescriptive guidance for hardening the DNS Server role. The DNS Server role has no subordinate role services.

Attack Surface

The DNS Server role is susceptible to many of the same security attacks as any server computer that provides DNS services. To determine the attack surface of this role service, you need to identify the following:

- **Installed files**. The files that are installed as part of the DNS Server role.
- **Running services**. The services that are installed as part of the DNS Server role.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The firewall rules that the DNS Server role uses.
- **Role dependencies**. The dependencies for the DNS Server role.

The details of the attack surface for the DNS Server role are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this server role, on the **DNS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your DNS Server role configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the DNS Server option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers performing the DNS Server role. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 5.1 Configuration Checklist

	Configuration tasks
	Deploy a Server Core installation of Windows Server 2008.
	Protect DNS zones in unsecured locations by using read-only domain controllers (RODCs).
	Combine the DNS and AD DS server roles on the same server.
	Configure zones to use secure dynamic updates.
	Restrict zone transfers to specific server computers running DNS.
	Deploy separate server computers for internal and external DNS resolution.
	Configure the firewall to protect the internal DNS namespace.
	Enable recursion to only the appropriate DNS servers.
	Configure DNS to ignore non-authoritative resource records.
	Configure root hints for the internal DNS namespace.

Deploy a Server Core Installation of Windows Server 2008

Deploying Windows Server 2008 using the Server Core installation option reduces the attack surface of the operating system by limiting the number of required files and services. The advantage of the Server Core option is that it does not install files and services required for the graphical user interface (GUI).

When you use the Server Core installation option of Windows Server 2008 to deploy the operating system, you can only locally manage the server using command-line tools. To manage the server using GUI-based tools, you must install and run these tools on another computer with a Windows-based GUI.

You can use the following command line management tools to manage the DNS Server role:

- To install the DNS Server role, run the following command:

  ```
  start /w ocsetup DNS-Server-Core-Role
  ```

- To configure the DNS Server service, run the following command:

  ```
  sc config dnsserver start = auto
  ```

  Note A space is required between "start" and "=". Also, a space is required between "=" and "auto".

- To start the DNS Server service, run the following command:

  ```
  net start dnsserver
  ```

- To configure DNS zones, run the following command:

  ```
  dnscmd
  ```

- To uninstall the DNS Server role, run the following command:

  ```
  start /w ocsetup DNS-Server-Core-Role /uninstall
  ```

For more information about installing and managing the DHCP Server role using the Server Core installation option, see the *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*. And for more information about managing DNS zones by using dnscmd, see the Dnscmd Overview on the Microsoft Windows Server TechCenter.

Protect DNS Zones in Unsecured Locations by Using RODCs

Because of their importance, Microsoft recommends physically securing the DNS servers in your environment in locations that are accessible only to qualified administrative staff. If your organization must provide DNS services in unsecured locations, such as branch office locations, protect the DNS zones using Active Directory Integrated zones replicated to RODCs.

RODCs contain a replicated, read-only copy of the application directory partitions that DNS uses to store Active Directory integrated zones, including the domain partition, ForestDNSZones and DomainDNSZones. This ensures that the DNS server running on the RODC has a read-only copy of any DNS zones stored on a centrally-located domain controller in those directory partitions. An administrator of a RODC can only view the contents of the read-only copy of the zone. However, an administrator can change the contents of the zone on a domain controller that has write access.

AD DS relies on DNS to provide name-resolution services to network clients. The changes to the DNS Server role service are required to support AD DS on a RODC.

Note Any computer stored in a location that is not physically secured represents a security risk to an organization.

Combine the DNS and AD DS Roles on the Same Server

Microsoft recommends to install the DNS Server role on the same server computer that performs the AD DS role in your environment. Combining these roles on the same server allows it to secure dynamic updates of DNS records.

However, Microsoft recommends to avoid combining the DNS Server role with server roles other that the AD DS role to minimize the attack surface of the server. Minimizing the attack surface of the DNS and AD DS roles on the same server computer is important, because the functionality of the entire forest or domain depends on the services this server performs.

In some smaller organizations, budget considerations compel administrators to combine roles. If this is required in your organization, you can combine a RODC and DNS with other server roles. Only RODCs allow the delegation of local administration of the computer without delegating administration of AD DS.

However, Microsoft recommends to only combine domain controllers with write access with the DNS Server role if you need to managed the DNS zones on the domain controller. This is because you cannot create writable versions of Active Directory Integrated zones on a RODC.

Configure Zones to Use Secure Dynamic Updates

Windows domains often include hundreds or thousands of DNS clients that must be registered, including servers, domain controllers, and workstations. Because maintaining these resources manually can be very time consuming, DNS supports dynamic updates. Dynamic updates ensure that the DNS client is responsible for its own updates, which also reduces administrative overhead.

However, dynamic updates can be used to attack a computer environment. Introducing rogue DNS clients to the network can fill the DNS database with false entries. Secure dynamic updates mitigate this risk by requiring all DNS clients to be members of the Windows Server 2008 domain. Secure dynamic updates require the server to use Active Directory with DNS. For this reason, you cannot take advantage of this security measure when DNS is installed on a stand-alone computer.

Restrict Zone Transfers to Specific Computers Running DNS

You can specify which servers can transfer zones. By default, any DNS server can transfer zone information to any other DNS server. However, you can restrict which servers can request zone transfer by modifying the properties of the DNS server.

Active Directory integrated zones replicates zones by using Active Directory replication, which keeps the zones more secure. Also, Active Directory automatically replicates to all other domain controllers in the domain. For this reason, you cannot restrict zone transfers for Active Directory Integrated zones.

However, in cases where zone information must traverse a public network, or where you cannot use AD DS domain controllers, you need to use another mechanism to limit zone transfers. One such option is to use IPsec for DNS server communication, which allows you to protect zone transfer information across the network.

Deploy Separate Server Computers for Internal and External DNS Resolution

Microsoft recommends to host your internal DNS namespace on DNS servers located behind the firewall of your network. Manage an external-facing DNS presence using a DNS server in a perimeter network (also known as DMZ, demilitarized zone, or screened subnet).

To provide Internet name resolution for internal hosts, you can configure your internal DNS servers to use a forwarder to send external queries to external DNS servers. A *forwarder* is a DNS server on a network that forwards DNS queries for external DNS names to DNS servers outside of that network. You can also forward queries according to specific domain names using conditional forwarders. For more information about forwarders, see the Using forwarders page on Microsoft TechNet.

Note In many environments there is no need for internal computers to resolve Internet-based names. And in situations where such computers need to resolve Internet-based names, a proxy server can resolve Internet-based names for internal computers. For more information about this topic, see Configuring DNS Servers for ISA Server 2004.

Microsoft recommends to configure your DNS servers to resolve queries on their own, instead of forwarding queries to untrusted DNS servers. However, in some instances, such as resolving domain name spaces for Internet-based hosts, this may not be possible. For the DNS servers in your network that are exposed to the Internet, restrict DNS zone transfers to either DNS servers identified in the zone by name server (NS) resource records, or to specific DNS servers in your network.

Configure the Firewall to Protect the Internal DNS Namespace

To prevent anyone outside of your organization from obtaining information about your internal DNS namespace, configure your routers and firewalls to only allow only outbound DNS traffic between your internal DNS servers and external DNS servers in an extranet or on the Internet. This configuration allows your internal DNS servers to forward DNS queries outward, but prevents external requests from being sent to your internal DNS servers. If you are using Microsoft Internet Security and Acceleration (ISA) Server, you can use block filters to define the traffic allowed through the ISA Server.

If your proxy server has two network interface cards (NICs)—one for the intranet and one for the Internet—and the proxy server is also performing the DNS Server role, you can configure the server to only listen for DNS traffic on the IP address that the intranet NIC uses.

Enable Recursion to Only the Appropriate DNS Servers

Only servers that respond to DNS clients directly need to have recursion enabled. DNS servers use iterative queries to communicate. Microsoft recommends disabling recursion on the DNS servers in your environment that do not respond to DNS clients directly, and that are not configured to use forwarders.

As an alternative, you can deploy the following types of DNS servers:

- Servers that host a specific set of names for other name servers to resolve.
- Servers that resolve names by finding an authoritative server.

To enable or disable recursion, on the **Advanced** tab of the **Properties** page of the DNS server, select the **Disable recursion** check box. For more information about this topic, see "Configure a DNS server to use forwarders" in the Help and Support for Windows Server 2008.

Configure DNS to Ignore Non-Authoritative Resource Records

DNS servers should ignore resource records from servers that are not authoritative for those records. Such nonauthoritative resource record information is known as *name pollution*. You can protect your DNS from name pollution by ensuring that the **Secure cache against pollution** check box on the **Advanced** tab of the DNS server properties dialog box is selected, which is the default configuration. Also ensure that the **Secure cache against pollution** check box is selected on all DNS servers in your environment.

Configure Root Hints for the Internal DNS Namespace

If you have a private internal DNS namespace and the computers on your intranet do not need to communicate with the Internet, configure the root hints on your internal DNS servers to only point to DNS servers that host your internal root domain, not the DNS servers that host the Internet root domain.

Relevant Group Policy Settings

Although there are Group Policy settings for the DNS Client service, there are no Group Policy settings available for the DNS Server service.

More Information

The following resources on Microsoft.com can provide you with further security best practice information about how to harden server computers that perform the DNS role:

- Configuring DNS Servers for ISA Server 2004.
- Dnscmd Overview.
- New features for DNS.
- *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.
- Using DNS Security Extensions (DNSSEC).
- Using forwarders.

Chapter 6: Hardening Web Services

This chapter focuses on how to harden Web servers running Windows Server® 2008. The Web Server role by default installs Microsoft® Internet Information Services (IIS) 7.0 on a computer running Windows Server 2008.

Microsoft redesigned IIS 7.0 into 40 modular components that you can choose to install as needed. The fewer components that you install, the smaller the attack surface that is available to a potential attacker.

By default, IIS 7.0 Setup installs a Web server with minimum functionality that supports static Web pages, request filtering, static file compression, and the IIS Manager GUI interface. There are many IIS 7.0 scenarios that organizations can use to provide Web services. However, the following two considerations are key to planning your Web server design:

- The sensitivity of the data that the server will present: Knowing this provides you with an idea of the risk involved if the data is compromised, and how much effort your organization should spend to protect it.
- The required user experience: Knowing this governs the feature requirements of the Web site itself, and the components that you need to install to secure it.

This chapter focuses on a typical scenario of a Web server hosted on a corporate intranet that displays mission critical content and data. Access to the server, or applications on the server, is restricted to users on a job need basis. This type of Web server requires authentication and authorization mechanisms that are tied to Active Directory® users and groups. You can use these groups to generate certificates to identify users after you have granted them permission to access information on the server.

For this scenario, this chapter discusses how you can apply best practice processes to harden your Web server against malicious attacks from either anonymous or authorized users. If you choose to use the default modules that install with IIS 7.0, these configure the Web server to only provide static HTML pages and images. The Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator lists the files and services that install with each feature.

As in previous versions of IIS, when you perform a default installation of IIS 7.0 on a computer running Windows Server 2008, the Setup program installs and starts the Worldwide Web Publishing (W3SVC) service on the server computer.

In addition, the IIS 7.0 Setup program installs and starts the Windows Process Activation Service (WAS). WAS generalizes the IIS process model, making IIS 7.0 HTTP independent. Because of this, your IIS server can now host Windows Communication Foundation (WCF) services using non-HTTP protocols. It also includes configuration application programming interfaces (APIs) that allow you to configure WAS settings programmatically. The W3SVC service depends on the WAS service.

Finally, the default installation of IIS 7.0 also installs the Application Host Helper Service (AppHostSvc). This service provides a configuration history feature that lets you go back to an earlier version of the Web server configuration. The Application Host Helper Service saves the ApplicationHost.config file to separate configuration history subdirectories at intervals that you specify. Previous configuration settings for this service were stored by default in the \inetpub\history\CFGHISTORY_*xxxxxxxxxx* subdirectory, where each x represents a number that would increment for each configuration version. If you copy an earlier version of the IIS configuration file into the %windir%\system32\inetsrv\config directory, you will return IIS to the configuration state contained in the restored file.

Secure By Default

At a conceptual level, the security considerations for the Web server role using IIS 7.0 on a computer running Windows Server 2008 have not changed significantly from those for a computer running IIS 6.0 with Windows Server® 2003. It remains important to keep the server's attack surface as small as possible.

However, at the implementation level, a lot has changed between the releases of IIS 6.0 and IIS 7.0. A fundamental change is that instead of installing a variety of features with IIS 6.0 and then having to enable or disable them, IIS 7.0 uses a minimum installation by default approach—only installing components that work with static sites. The default installation for IIS 7.0 includes the following feature modules:

- Static content module
- Default document module
- Directory browsing module
- HTTP Errors module
- HTTP Logging module
- Request Monitor module
- Request Filtering module
- Static Content Compression module
- IIS Management Console module

The default installation of IIS 7.0 does not support ASP.NET or ASP functionality. You must explicitly select them during the role selection process to include these technologies on your IIS 7.0 Web server. The following figure illustrates the role services that make up the Windows Server 2008 Web Server (IIS) role.

Note The items in bold in the figure are components that install by default when you select the high-level Web Server role.

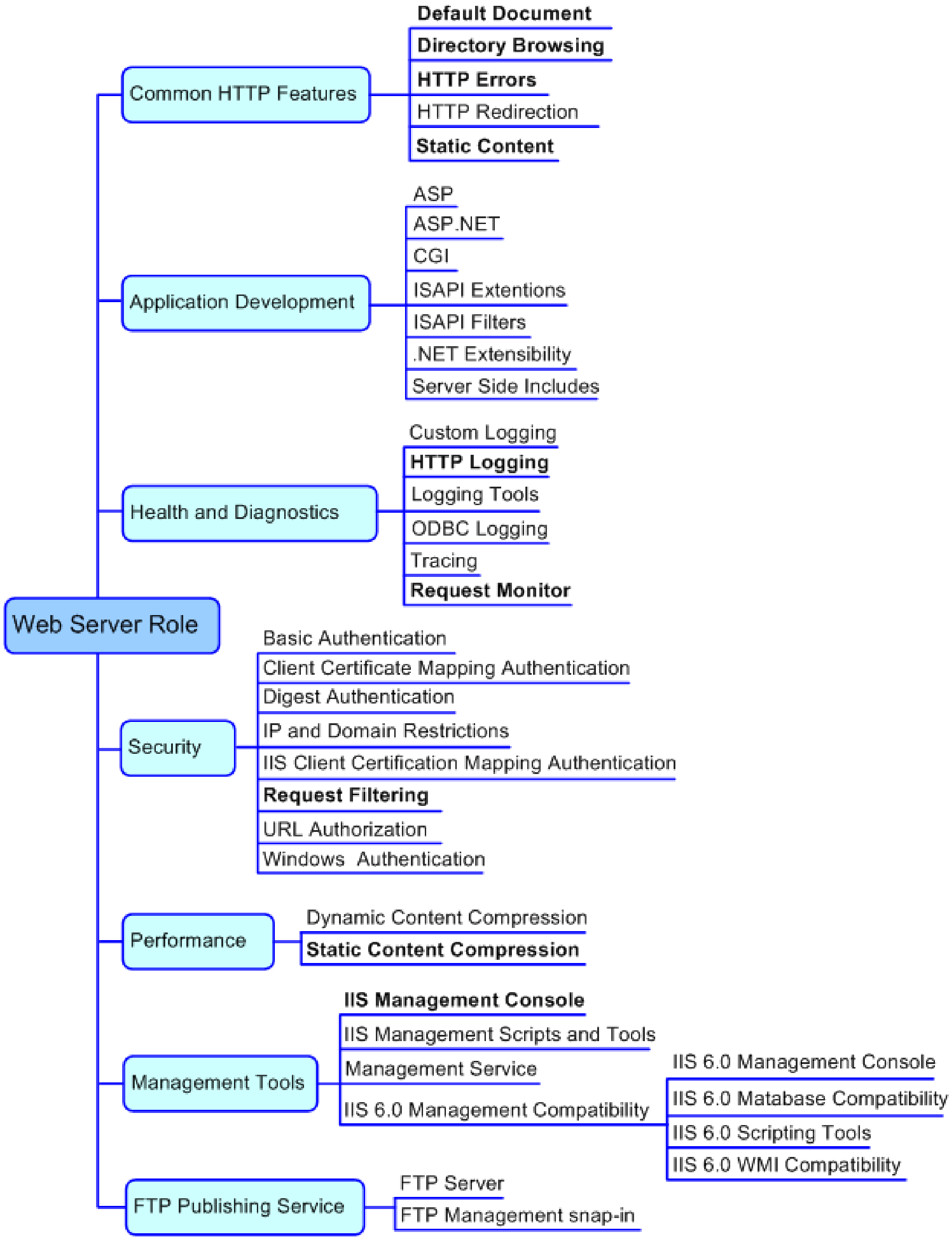


Figure 6.1 Role services hierarchy for the Web Server role

Attack Surface

Microsoft designed IIS 7.0 with a modular architecture and a minimum of module and feature dependencies. You can choose from 40 modules to customize your installation for the needs of your particular Web server.

The default installation of IIS 7.0 only supports serving static content such as HTML and image files. This exposes the minimum attack surface while still providing Web server functionality.

Microsoft organized the IIS 7.0 installation into seven feature areas. These include the Common HTTP Features feature area, the Application Development feature area, the Health and Diagnostics feature area, the Security feature area, the Performance feature area, the Management Tools feature area, and the FTP Publishing Service feature area. How you want to manage your IIS 7.0 Web server and the feature requirements of the sites and applications that you plan to host on your IIS 7.0 Web server determines which modules and features to install. However, the more modules and features that you install, the larger the attack surface on the Web server.

The IIS 7.0 setup program installs a different set of files, services, and firewall rules based on the features and modules that you choose. To determine the attack surface of this role service, you need to identify the following:

- **Installed files**. The files that are installed as part of the Web Server role.
- **Installed services**. The services that are installed as part of the Web Server role.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The firewall rules that are installed (or enabled) for the Web Server role.

The details of the attack surface for the Web Server role are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **Web** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes security measures that you can incorporate into your Web server (IIS) configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Web Server role on the **Select Role Services** page of the Add Roles Wizard, accepted all of the defaults, and included the ASP.NET option. Further recommendations for the Common HTTP Features, Application Development, Health and Diagnostics, Security, Performance, Management Tools, and FTP Publishing services are not included. For more information about how to configure these services, see IIS 7.0: Configure Web Server Security.

There are many ways to set up a Web server that uses IIS, but this guidance focuses on a common scenario that uses an ASP.NET application that connects to a database. For example, an internal ordering system or a Human Resource application could provide such a database.

A Web site of this type typically consists of the following:

- Static pages (HTML pages).

- Images that use .jpg and .gif file formats.
- Dynamic ASP.NET pages.

As part of planning the installation for the Web server, ensure that the application developers in your organization follow security best practices. For more information about best practices in this area, see Improving Web Application Security: Threats and Countermeasures.

It is important to understand that if your organization does not follow security best practices, you will be making it easy for your Web server to fall victim to malicious attacks. Even after using security best practices to set up a Web application, there are several steps that you need to take to secure the Web server.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers that perform the Web Server role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 6.1 Configuration Checklist

	Configuration tasks
	Consider deploying a Server Core Installation of Windows Server 2008.
	Install the application development environment.
	Set the authentication mechanism.
	Remove unused IIS components.
	Configure a unique binding.
	Move root directories to a separate data partition.
	Configuring user account permissions.
	Enable Secure Sockets Layer (SSL).
	Consider additional specialized security configuration measures.

Consider Deploying a Server Core Installation of Windows Server 2008

Consider deploying Windows Server 2008 using the Server Core installation option to further reduce the attack surface of the operating system by reducing the number of installed files and running services. The advantage of the Server Core installation option is that a graphical user interface (GUI) is not installed, so the files and services required by the normal GUI are not installed.

There are two issues you need to be aware of when using a Windows Server 2008 Server Core installation for the Web Server (IIS) role. First, you cannot directly manage the installation using a GUI. Instead you must use the Microsoft Management Console (MMC) management tools remotely from a computer that has them installed or use command-line management tools to directly manage the server installation. Second, Server Core does not support ASP.NET and .NET Framework associated features. If your applications require .NET functionality, you cannot use the Windows Server 2008 Server Core installation.

Because the scenario used in this chapter requires ASP.NET, you cannot attempt these procedures using a Server Core installation. However, apply the general principles outlined to any Web Server (IIS) role using a Server Core installation.

You can use the following command-line management tools to install the Web Server role on computer running Windows Server 2008:

- To install the default Web Server (IIS) role and the services associated with it, complete the following command:

  ```
  start /w pkgmgr /iu:IIS-WebServerRole;WAS-
  WindowsActivationService;WAS-ProcessModel
  ```

- To install all available services and features for the Web Server (IIS) role, complete the following command:

  ```
  start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-
  CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-
  DirectoryBrowsing;IIS-HttpErrors;IIS-HttpRedirect;IIS-
  ApplicationDevelopment;IIS-ASP;IIS-CGI;IIS-
  ISAPIExtensions;IIS-ISAPIFilter;IIS-ServerSideIncludes;IIS-
  HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-
  RequestMonitor;IIS-HttpTracing;IIS-CustomLogging;IIS-
  ODBCLogging;IIS-Security;IIS-BasicAuthentication;IIS-
  WindowsAuthentication;IIS-DigestAuthentication;IIS-
  ClientCertificateMappingAuthentication;IIS-
  IISCertificateMappingAuthentication;IIS-URLAuthorization;IIS-
  RequestFiltering;IIS-IPSecurity;IIS-Performance;IIS-
  HttpCompressionStatic;IIS-HttpCompressionDynamic;IIS-
  WebServerManagementTools;IIS-ManagementScriptingTools;IIS-
  IIS6ManagementCompatibility;IIS-Metabase;IIS-
  WMICompatibility;IIS-LegacyScripts;IIS-
  FTPPublishingService;IIS-FTPServer;WAS-
  WindowsActivationService;WAS-ProcessModel
  ```

For more information about how to install the Web Server (IIS) role with a Windows Server 2008 Server Core installation, see *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.

In addition, you can use the appcmd command-line tool to manage the Web Server role. For instructions on how to use the appcmd command-line tool, see the Administrative Tools section of the *IIS 7.0: Operations Guide* in the Windows Server 2008 TechNet Library.

You can also use WMI to locally or remotely manage the Web Server (IIS) role running on Windows Server 2008 Server Core installations.

For more information about WMI, see Windows Management Instrumentation and the WMI Section of the *IIS 7.0 Operations Guide* in the Windows Server 2008 TechNet Library.

Install the Application Development Environment

The scenario tested in this chapter uses ASP.NET because it is the most popular application development infrastructure that IIS provides. ASP.NET uses .NET Framework 2.0, which is available in Windows Server 2008.

In the **Select Role Services** section of the installation process for the Web server, when you select ASP.NET, the following IIS 7.0 components are required:

- **ASP.NET**: Includes files and configuration settings to enable ASP.NET on IIS.
- **ISAPI Filters**: ASP.NET requires an ISAPI Filter with the name "ASPNET_FILTER.DLL".
- **ISAPI Extensions**: The core functionality of ASP.NET is in the ASPNET_ISAPI.DLL file. This DLL file is built on top of the ISAPI Extension interface. IIS does not install the ISAPI Extension interface by default.
- **.NET Extensibility**: .NET extensibility allows your server to support managed modules that run using the ASP.NET programming model. Your developers can use .NET Framework APIs to create new Web server features.
- **WAS .NET Environment**: This supports managed code activation in the IIS 7.0 process model.

  If your ASP.NET applications are designed to use the out-of-process ASP.NET Session state service, you must enable this feature. If you have enabled this feature and your ASP.NET applications do not use it, disable it.

After installing the development environment, the next step to securing your Web server is to install the authentication mechanism that you want to use to determine the identity of users who connect to the applications on the Web server.

Set the Authentication Mechanism

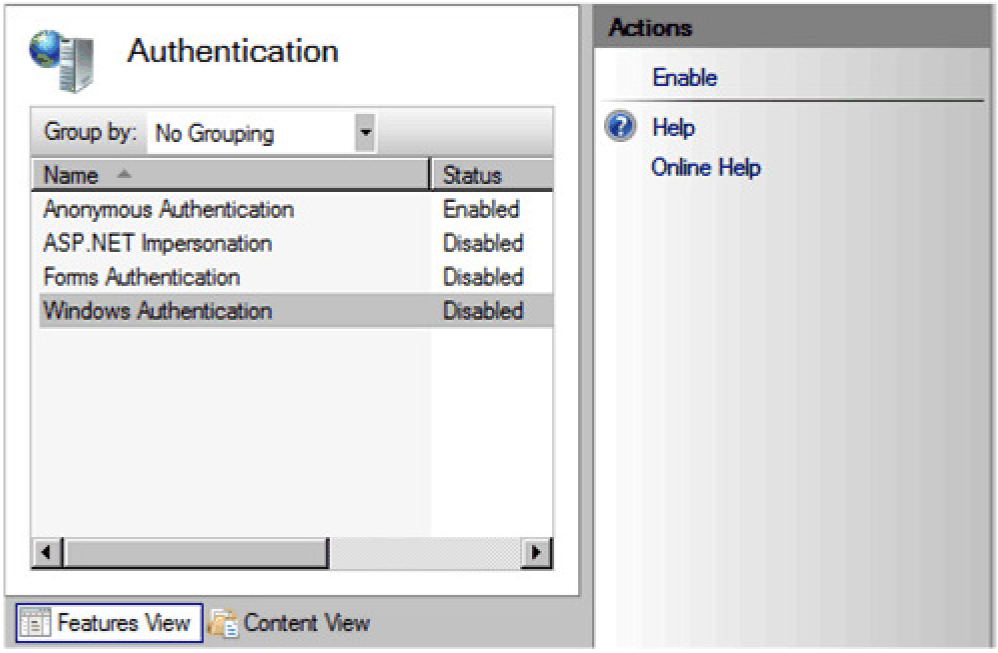
Microsoft recommends using Windows Authentication for Web applications as your user authentication mechanism because it is integrated with Windows and Active Directory Domain Services (AD DS). By turning Windows Authentication on and Anonymous Authentication off, only authenticated users can access Web applications. You can use the following procedures to install, enable, and disable these authentication mechanisms.

To install Windows Authentication

1. Click **Start** and then click **Server Manager**.
2. In the **Server Manager** pane, expand **Roles**, and then click **Web Server (IIS)**.
3. In the **Role Services** box, click **Add Role Services**.
4. In the **Add Role Services** wizard, select **Windows Authentication**, and then click **Next**.
5. On the **Confirm Installation Selections** page, click **Install**.
6. On the **Installation Results** page, click **Close**.

To enable Windows Authentication

1. In the **Server Manager** pane, click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, click the server name, and then in the **Home** pane, double-click **Authentication**.



Name	Status
Anonymous Authentication	Enabled
ASP.NET Impersonation	Disabled
Forms Authentication	Disabled
Windows Authentication	Disabled

Figure 6.2 Enabling Windows Authentication in IIS Manager

3. In the **Authentication** pane, click **Windows Authentication**, and then in the **Actions** pane, click **Enable**.

To disable Anonymous Authentication

1. In the IIS Manager **Authentication** pane, click **Anonymous Authentication**.
2. In the **Actions** pane, click **Disable**.

Important This procedure turns Anonymous Authentication off for the entire IIS Web Server. If you have other Web applications that need anonymous access you might have to turn the setting back on for those Web applications.

It is also possible to disable Anonymous Authentication using the command line. This can be useful when using a script to configure the Web server.

To disable Anonymous Authentication via the command line, at the command prompt, use the following syntax:

```
%windir%\system32\inetsrv\appcmd set config –
section:anonymousAuthentication –enabled:false
```

Remove Unused IIS Components

At this point in the Web Server role configuration process, review the IIS 7.0 components installed on the server to ensure that all of those that your installation requires are present. You must explicitly install all role services and features provided by IIS 7.0. The only way a service you do not need can install on your Web server is if you install it. Refer to the "Attack Surface" section earlier in this chapter to determine the role services that your Web server requires, add any that your applications require, and remove any that you do not require.

Some typical areas in which to check for components include:

- Default Common HTTP modules installed by the IIS 7.0 Setup program.
- Unused development environments.
- Management features.

Configure a Unique Binding

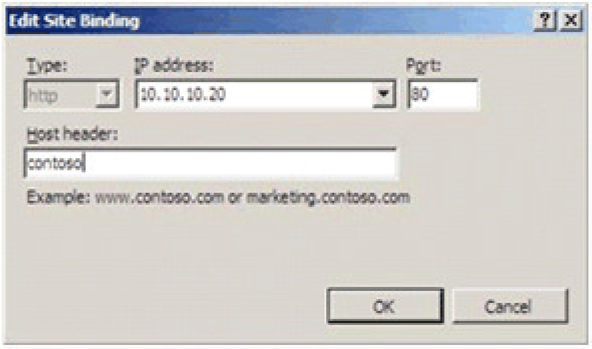
By default, the IIS Web site listens on all configured IP addresses of the Web server for connections. The site also serves all requests that use port 80, regardless of the host header specified. Malicious software, such as viruses or worms, can attempt to iterate through a range of IP addresses to find new Web servers to infect. You can reduce the risk or such attacks by configuring the default Web site to only listen to a specific host name, which is called a unique binding.

For example, if you configure a host name as, *:80:myWebServer, instead of listening to all host names (*:80:*), such a configuration can prevent automated attacks that only use an IP address to attempt to access a server. An automated attack would usually attempt to iterate through the IP address namespace. For example, it could first try 1.1.1.1, then 1.1.1.2, 1.1.1.3, and so on.

Without a host name configured as a unique binding, your Web site would eventually receive a network packet from the attack. However, if you configure the server to require a host name, the automated attack will fail because the request to the IP address will fail, and the worm cannot determine the host name of the server without including more complex code to resolve host names. You can use the following procedure to configure a unique binding.

To configure a unique binding

1. Open **Internet Information Services (IIS) Manager**.
2. Select the name of your Web server, and then under the **Sites** node, right-click the required Web site.
3. From the context menu select **Edit Bindings**.
4. In the **Edit Site Binding** dialog box, select **http** in type list, and then click **Edit**.
5. Select the required IP address for the server's Web site, and then configure the Host header to match your required host name as shown in the following figure.



Type: http

IP address: 10.10.10.20

Port: 80

Host header: contoso

Example: www.contoso.com or marketing.contoso.com

Figure 6.3 The Edit Site Binding dialog box

Based on the information in the previous figure, only applications that request the full URL for "http://contoso" can access the site. If an automated Internet worm tries to access the site using an IP address, for example "http://10.10.10.20," the connection attempt will fail.

You also can configure this setting from a command line using the following syntax:

```
%windir%\system32\inetsrv\appcmd set site "Default Web Site" -
bindings:http/10.10.10.20:80:contoso
```

Move Root Directories to a Separate Data Partition

Past security vulnerabilities allowed an attacker to traverse from the URL namespace into the file system directories of the operating system. For example, if http://contoso/cgi.exe mapped to C:\inetpub\wwwroot\cgi.exe, without safeguards, an attacker could use the URL to execute the Windows command processor cmd.exe instead of the CGI program cgi.exe to access the following location:

http://contoso/../../windows/system32/cmd.exe.

IIS 7.0 is designed to prevent this type of attack by default. However, it is a best practice to move your Web site content on to a separate data partition from the one that the operating system uses. Although not required, many organizations choose to store Web site content on a dedicated data partition. This can provide both performance and security benefits. The following steps explain how to move Web site content to a new partition.

To move Web site content to a new partition

1. Open **Internet Information Services (IIS) Manager**.
2. Click the name of your Web server, and then underneath **Sites**, right-click **Default Web Site**.
3. Select **Manage Web Site**, and then select **Advanced Settings**.
4. Change the **Physical Path** property to a directory on the new data partition.

This process does not move the Web site's content or change the permission for the Web folder, so you also must transfer those resources across to complete the move.

You can change the default physical path for the Web site by executing the following command line:

```
%windir%\system32\inetsrv\appcmd set vdir "Default Web Site/" -
physicalPath:D:\Web
```

Note This command assumes your new Web site content directory is D:\Web.

Configuring User Account Permissions

Next, you must assign permissions on the Web site content directory and check the user accounts that will be allowed access to the Web site. To do this, grant access to the following security entities:

- The account associated with the IIS worker process used for the Default Web Site.

  By default, this is the NetworkService account. You must edit the Default Application Pool configuration settings to change this default. If you have changed this setting to a custom account, you must grant access to the custom account, not the NetworkService account.

Note Do not change the account to the LocalSystem or LocalService account. Each of these accounts have more permissions that Microsoft recommends to grant to IIS worker processes.

- The users who access your Web site.

  In most cases, you can keep the default ComputerName\Users group permissions for the folder, which allows members of a domain to access the content folder. If there are any special permissions granted to the ComputerName\Users group, ensure to remove them.

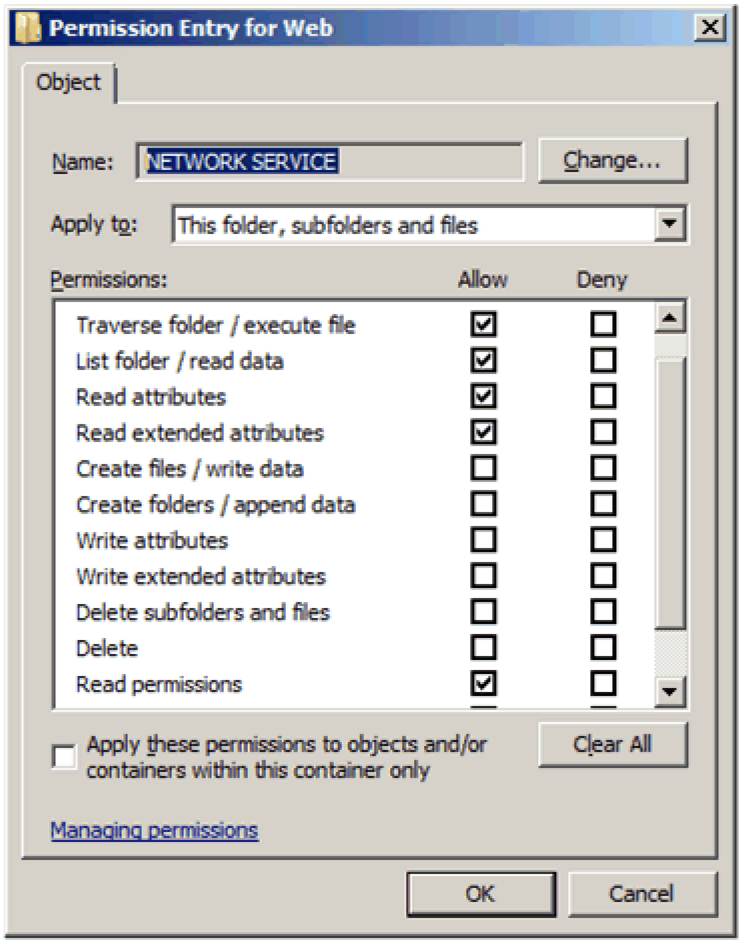
- The Web site administrators.

To configure the permissions for the Web site, you use the standard Windows file system permissions mechanism via Windows Explorer. This allows you to determine the exact security permissions for each security entity. You can use the following procedure to achieve this.

To set permissions on the D:\Web folder

1. Open **Windows Explorer**, right-click the Web content folder (D:\Web in the example in this chapter), and then click **Properties**.
2. Click the **Security** tab, click the **Advanced** button, and then select **Edit**.
3. Clear the checkbox for **Include inheritable permission from this object's parent**.
4. In the **Windows Security** dialog box, select the **Copy** checkbox to copy the inherited permission to the folder.
5. Select the checkbox for **Replace all existing inheritable permissions on all descendants with inheritable permissions from this object**.

6. Select each permission entry, and then click **Remove**, except for the following:
    - **SYSTEM**
    - **Administrators**
    - <*ComputerName*>**Users**, for example WebServer1\Users
7. Click **Add**, and then in **Enter the object name to select** box, type **Network Service**.
8. Click **Check Names** to resolve the **NETWORK SERVICE** name. This is the IIS default worker process identity.
9. Click **OK**, then confirm that the list of permissions displayed in the following figure is selected under **Allow** in the **Permission Entry** box, and then click **OK**.



Name: NETWORK SERVICE

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse folder / execute file	☑	□
List folder / read data	☑	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / write data	□	□
Create folders / append data	□	□
Write attributes	□	□
Write extended attributes	□	□
Delete subfolders and files	□	□
Delete	□	□
Read permissions	☑	□

□ Apply these permissions to objects and/or containers within this container only

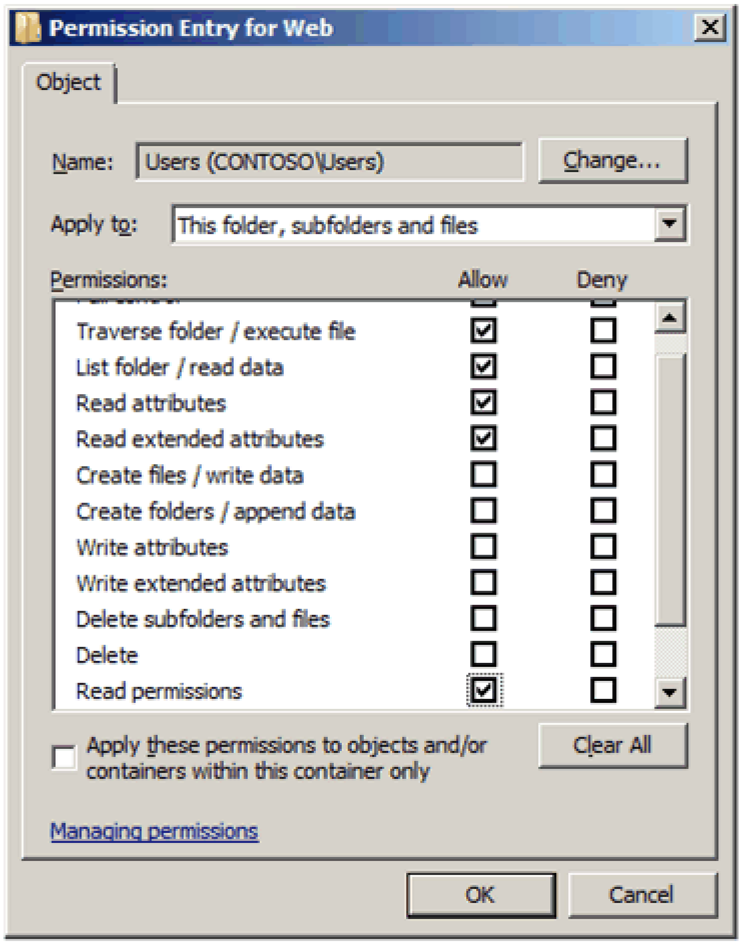
Figure 6.4 Setting ACLs for the Network Service Account

10. On the **Advanced Security Settings** dialog box, click **Add**, and then in the **Enter the object name to select** box, type <*DomainName*>**Users**.

    For the Contoso domain this example uses, you would type Contoso\Users.
11. Click **Check Names** to resolve the **Domain Users** name.

    Note These are the users who you are allowing access to the Web site. For a site that has special security requirements, you may wish to assign permissions to a dedicated user group that contains users who are specifically added to the group as required. If possible, maintain the MachineName\Users group with read and execute permissions.

12. Click **OK** and then ensure that permissions are selected in the **Permission Entry for Web** dialog box as displayed in the following figure. Finally, click **OK** as needed to exit the **Properties** window.



Permission Entry for Web

Name: Users (CONTOSO\Users)

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse folder / execute file	☑	□
List folder / read data	☑	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / write data	□	□
Create folders / append data	□	□
Write attributes	□	□
Write extended attributes	□	□
Delete subfolders and files	□	□
Delete	□	□
Read permissions	☑	□

□ Apply these permissions to objects and/or containers within this container only

Figure 6.5 Setting ACLs for domain users

Enable Secure Sockets Layer (SSL)

If the network communications between the Web server and the client computers passes over untrusted networks, Microsoft recommends to enable Secure Sockets Layer (SSL) to encrypt the traffic to help secure it from network sniffing and host spoofing.

SSL requires a certificate that proves the servers identity and that is trusted by the client browsers. If the Web server can only be accessed privately within the enterprise, this certificate can be obtained from the organization's existing public key infrastructure (PKI). However, if the Web server can be accessed from the Internet, Microsoft recommends to obtain a certificate from a public certificate authority. For testing purposes, you can also use a self-signed certificate to encrypt traffic.

IIS 7.0 supports several methods to install a SSL certificate including:

- Using the IIS Manager GUI.
- Using the Certificate Manager GUI.
- Web and Auto-enrollment.
- Using the appcmd command-line tool.
- Programmatically through Microsoft.Web.Administration using Windows Management Instrumentation (WMI) scripts.

For more information about how to install a SSL certificate, see the How to Setup SSL on IIS 7.0 page on the Microsoft Internet Information Services (IIS) Web site.

Installing the SSL certificate hardens your Web server configuration to a level that provides elevated security while ensuring that you can manage a functional feature set for the server.

Consider Additional Specialized Security Configuration Measures

For environments that require added security, there are a few additional measures that you can take to further harden the Web server. However, it is important to note that these steps do increase management overhead and can create Web application compatibly issues. It is very important to conduct thorough testing of your Web applications in a test environment before attempting to implement these recommendations on a production server.

To further secure your Web server installation, you might consider using the following features:

- Access control list (ACL) hardening. You can further limit access to your Web site by specifying particular users in the ACL for your content directory instead of allowing all domain users to access the site.
- If you want a more user friendly feature to limit access to your Web site, you can use the built-in IIS7 URL Authorization feature. For more information about this feature, see the Understanding IIS7 URL Authorization page on the Microsoft IIS Web site.
- The IPv4 Restriction Lists feature, which lets you restrict the IP addresses of the client browsers you allow to connect to the Web server.
- The Request Filtering feature, which lets you control many HTTP features, such as HTTP verbs, HTTP headers and URL size. For more information about this feature, see the How to Use Request Filtering page on the Microsoft IIS Web site.

- Client certificate mapping, which allows you to enforce strong authentication by requiring users to provide client certificates when requesting to access your site. For more information about this feature, see the How to Setup SSL on IIS 7.0 page on the Microsoft IIS Web site.

You can also change the site's identity by changing the Application Pool identity to a low privileged local account.

More Information

The following resources on Microsoft.com can provide you with further security best practice information about how to design and maintain Web servers:

- *Antivirus Defense-in-Depth Guide*.
- How to Setup SSL on IIS 7.0.
- How to Use Request Filtering.
- Improving Web Application Security: Threats and Countermeasures.
- IIS 7.0: Configure Web Server Security.
- *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.
- Windows Management Instrumentation.
- Windows Server 2008 TechNet Library.
- "Virus scanning recommendations for computers that are running Windows Server 2003, Windows 2000, Windows XP, or Windows Vista": Knowledge Base article 822158.
- Understanding IIS7 URL Authorization.

Chapter 7: Hardening File Services

This chapter focuses on how to harden computers that perform the File Services role service available in Windows Server® 2008. Computers that perform this role can provide a particular challenge to harden, because balancing the security and functionality of the fundamental services that they provide is a fine art. Windows Server 2008 introduces a number of new features that can help you to control and harden the File services in your environment.

Server Message Block (SMB) is the file-sharing protocol that Windows®-based computers use by default. SMB is an extension of the Common Internet File System (CIFS). Windows Server 2008 features SMB version 2.0, which provides enhanced performance.

You can configure and apply most of the policy settings this chapter discusses through Group Policy. You can link a Group Policy object (GPO) that complements the Member Server Baseline Policy (MSBP) to the appropriate organizational units (OUs) that contain computers running Windows Server 2008 that perform the File Services role. Doing this provides the required security settings for this server role. This chapter only discusses Group Policy settings that vary from those for the MSBP.

The File Services role service also allows you to install the Distributed File System (DFS) role service. DFS consists of the following two technologies that you can use together or independently to provide fault-tolerant and flexible file sharing and replication services on a Windows-based network:

- **DFS Namespaces**. This technology enables you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. However, the underlying structure of the namespace can consist of numerous shared folders located on different servers and in multiple sites. Because the underlying structure of shared folders is hidden from users, a single folder in a DFS namespace can correspond to multiple shared folders on multiple servers. This structure provides fault tolerance and the ability to automatically connect users to local shared folders, instead of routing them over wide area network (WAN) connections.
- **DFS Replication**. This technology is a multimaster replication engine that enables you to synchronize folders on multiple servers across local or WAN network connections. This service uses the Remote Differential Compression (RDC) protocol to update only the portions of files that have changed since the last replication. You can use DFS Replication in conjunction with DFS Namespaces or by itself.

In addition, you can install the File Server Resource Manager (FSRM) role service, which provides a suite of tools that enables administrators to understand, control, and manage the quantity and type of stored data that the File services use. By using FSRM, you can place quotas on folders and volumes, actively screen files, and generate comprehensive storage reports.

The Services for Network File System (NFS) role service provides another file sharing solution for an enterprise that has a mixed Windows and UNIX environment. With

Services for NFS, you can transfer files between computers running Windows Server 2008 and UNIX operating systems using the NFS protocol. The Windows Search Service also enables you to perform fast file searches on a server from client computers that are compatible with Windows Search.

The Windows Server® 2003 File Server role provides the following services to Windows Server 2008 file servers to make them compatible with file servers running Windows Server 2003 and Windows® 2000:

- **File Replication Service (FRS)**, which supports synchronizing folders with file servers that use FRS instead of the newer DFS Replication service. To enable a server to synchronize folders with servers that use FRS with the Windows Server 2003 or Windows 2000 implementations of Distributed File System, install FRS. To enable the latest and most efficient replication technology, install DFS Replication.
- **Indexing Service**, which catalogs the contents and properties of files on local and remote computers. This service also enables you to quickly find files through a flexible query language. You cannot install Indexing Service and Windows Search Service on the same computer.

You can also install the following optional subelements for the File Services role:

- **Windows Server Backup**, which helps you reliably back up and recover the operating system, Windows Server System™ applications, and files and folders stored on the server. This sub-element introduces new backup and recovery technology, and replaces the previous Backup feature available in earlier versions of Windows.
- **Storage Manager for SANs**, which enables you to provision Fibre Channel or iSCSI storage subsystems on a storage area network (SAN).
- **Multipath I/O**, which allows you to increase data availability by providing redundant connections to storage subsystems. Multipathing can also provide load balancing of I/O traffic to improve system and application performance.

The following figure illustrates the role services that make up the Windows Server 2008 File Services role.

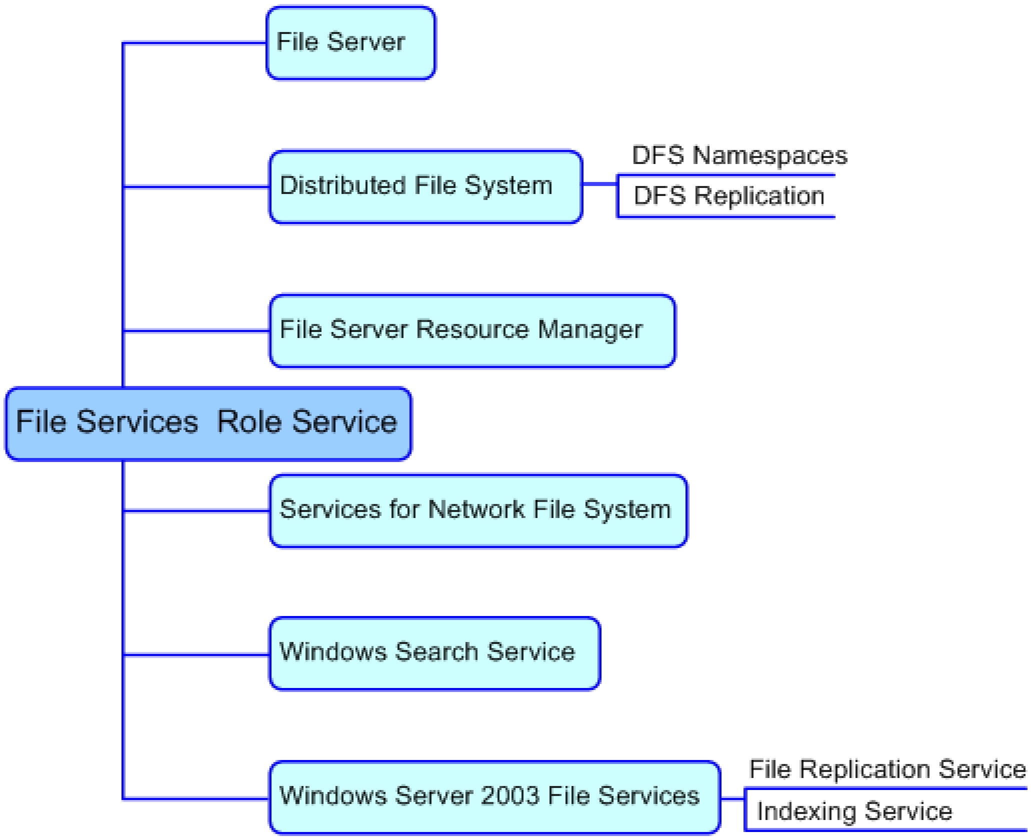


Figure 7.1 Role services hierarchy for the File Services role

Attack Surface

The File Services role provides technologies for storage management, file replication, distributed namespace management, fast file searching, and streamlined client access to files. To determine the attack surface of this role service, you need to identify the following.

- **Installed files.** The files that are installed as part of the File Server role.
- **Installed services.** The services that are installed as part of the File Server role.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules.** The firewall rules that the File Server role uses.

The details of the attack surface for the File Services role are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this server role, on the **File** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your File Server role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the File Server role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

This section includes configuration recommendations and a checklist based on best practices to further harden the File servers in your environment. Recommendations for the DFS, FSRM, Services for Network File System, Windows Search Service, and Windows Server 2003 File Services role services are not included. For more information about how to configure these services, see File Services in the Windows Server 2008 TechNet Library.

While these configuration changes help to protect your File servers against these threats, Microsoft recommends using additional antivirus protection to ensure that the File servers in your organization have real-time monitoring of files transferred through these servers. For more information about real-time antivirus protection for Windows Server 2008, see Security and Protection in the Windows Server 2008 TechNet Library.

The following table summarizes the recommended security configuration tasks for hardening servers performing the File Server role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 7.1 Configuration Checklist

	Configuration tasks
	Deploy a server core installation of Windows Server 2008.
	Digitally sign communications.
	Consider removing administrative shares.
	Consider using encryption for drives and files.

Deploy a Server Core Installation of Windows Server 2008

Deploying Windows Server 2008 using the Server Core installation option further reduces the attack surface of the operating system by reducing the number of installed files and running services. The advantage of the Server Core installation option is that a graphical user interface (GUI) is not installed, so the files and services required by the normal GUI are not installed.

When you use the Server Core installation option of Windows Server 2008 to deploy the operating system, you can only locally manage the server using command-line tools. To manage the server using GUI-based tools, you must install and run these tools on another computer with a Windows-based GUI.

The Server service installs and starts by default when you create a Windows Server 2008 Server Core installation and this service supports the File Server role service. If you need to install other services associated with the File Services role on a computer running a Server Core installation of Windows Server 2008, see the *Server Core Installation Option of Windows Server 2008 Step-by-Step Guide*.

You can use the following command-line tools to manage the File Server role services:

- net share
- chkdsk
- chkntfs
- dfsutil
- diskpart
- fsutil
- vssadmin

This is a partial list. For a complete list of command line tools and information about how to use them, see the "Command Reference" section of the Windows Server 2008 TechNet Library.

You can also use WMI scripts or WS-Management and the Windows Remote Shell to remotely manage File Services role services on computers running Windows Server 2008 Server Core installations.

For more information about WMI, see Windows Management Instrumentation.

For more information about WS-Management and the Windows Remote Shell, see Windows Remote Management.

Note This rest of this section assumes that you are running a standard installation of Windows Server 2008. If you have installed Windows Server 2008 Server Core for your File Server role, you can follow these steps using the Microsoft Management Console (MMC) snap-in from a remote computer.

Digitally Sign Communications

The SMB protocol provides the basis for Microsoft file and print sharing, and many other network operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports SMB packet digital signing. You can configure the Group Policy setting for **Microsoft network server: Digitally sign communications (always)** in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted. The setting for **Microsoft network server: Digitally sign communications (always)** is set to **Disabled** by default in Windows Server 2008. Microsoft recommends to enable this setting for files servers running in the EC and SSLF environments defined in this guide.

For more information about this security setting, see Microsoft network server: Digitally sign communications (always).

Consider Removing Administrative Shares

Windows Server 2008 creates by default a number of shares that are only accessible to users with administrator user rights on the File Server role service computer. For a File server with a single hard disk drive running the File Server role service, the following table defines these shares.

Table 7.2 File Server Administrative Shares

Share	Description	Path
Admin$	A share that an administrator uses to perform remote administration on a computer.	C:\Windows
DriveLetter$	Root partitions and volumes are shared as the drive letter name appended with the $ character.	C:\

For each additional volume on the server that you create, Windows Server 2008 creates a corresponding share of the volume root to make it available over the network to administrators.

In general, Microsoft recommends not to modify these special shares. However, if your organization has specific security requirements to remove these default folder shares, and prevent the operating system from automatically creating them, you can perform the following procedure by using the Registry Editor.

Caution If you use the Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk.

To remove administrative shares and prevent automatically creating them in Windows

1. Click **Start**, click **Run**, and then in the **Open** box, type **regedit** and press ENTER.
2. If you receive a User Access Control warning, click **Continue**.
3. Locate, and then click the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanSer
   ver\Parameters\AutoShareServer
   ```

   Note If the registry key is not listed, add it manually. AutoShareServer must be set as type REG_DWORD. When you set the value of this key to 0 (zero), Windows Server 2008 does not automatically create administrative shares. This does not apply to the IPC$ share or shares that you create manually.
4. On the **Edit** menu, click **Modify**, and then in the **Value** data box, type **0**, and click **OK**.
5. Quit the Registry Editor.
6. Click **Start**, and then click **Run**.
7. In the **Open** box, type **cmd** and then click **OK**.
8. At the command prompt, type the following lines, and press ENTER after each line:

   ```
   net stop server
   net start server
   ```

9. Type **exit** and then press ENTER.

Note If you use the user interface to stop the administrative shares and do not modify the registry, the shares will start again once you restart the Server service or if the server is reset.

Consider Using Encryption for Drives and Files

For environments with elevated security requirements, consider using encryption to secure the hard disk drives and data on your Windows Server 2008 computers performing the File Server role service. You can use one of two options for this on computers running Windows Server 2008 that perform the File Server role service:

- Microsoft BitLocker™ Drive Encryption.
- Encrypting File System (EFS).

BitLocker protects data on the server by preventing unauthorized users from breaking Windows file and system protection on lost or stolen computers. BitLocker encrypts entire volumes, including all user and system files, and within those files the swap and hibernation files.

For more information about how to use BitLocker to protect data on a computer running the File Server role service, see Windows BitLocker Drive Encryption.

EFS enables you to encrypt files stored on volumes that use the NTFS file system. EFS is integrated with NTFS, is easy to manage, and is difficult to attack. EFS enhancements in Windows Vista® and Windows Server 2008 include improvements in manageability and support for storing encryption keys on smart cards.

For more information about how to use EFS to protect data on your computer running the File Server role service, see Encrypting File System.

More Information

The following resources on Microsoft.com can provide you with more security best practice information about how to design and maintain a server running Windows Server 2008 that performs the File Server role:

- *Antivirus Defense-in-Depth Guide*.
- Encrypting File System.
- Microsoft network server: Digitally sign communications (always).
- Security and Protection.
- *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.
- "Virus scanning recommendations for computers that are running Windows Server 2003, Windows 2000, Windows XP, or Windows Vista": Knowledge Base article 822158.
- Windows BitLocker Drive Encryption.
- Windows Management Instrumentation.
- Windows Remote Management.
- Windows Server 2008 TechNet Library.

Chapter 8: Hardening Print Services

This chapter focuses on how to harden computers that perform the Print Server role available in Windows Server® 2008. Microsoft introduced significant security changes to printing services in the operating system for Windows Vista®. These changes also are incorporated into Windows Server 2008. For more information about the new features introduced in Windows Vista, see the "Point and Print Security in Windows Vista" white paper.

While the Printer service in Windows Server 2008 supports legacy clients, your organization cannot achieve optimal security unless all the client computers that you manage are running Windows Vista.

There are three role services that you can select to comprise the Print Server role on a computer running Windows Server 2008: the Print Server Role, the Line Printer Daemon (LPD) Service role service, and the Internet Printing role service.

- **Print Server role service**. Installing this role service makes very few changes to the server. The primary printing service is the Print Spooler service (Spooler). This service provides the majority of the functionality required for applications to manage printer related functions. In addition to managing the printer, many applications also rely on this service to assist in print and page operations, such as formatting pages as they display on screen. For this reason, the Print Spooler service is enabled by default in Windows Server 2008, regardless of whether the Print server has the printer service role installed or not. However, by default the service is not enabled for network access so you can only use it directly on the server console. This helps to reduce the attack surface on servers that are not actively sharing printers on the network.

  When you add the Print Server role service to a default installation of Windows Server 2008, and then install and share a print device, the Spooler and Server services become available for network connections by using remote procedure call (RPC). This change expands the attack surface of the Print server after these services become available over the network.

  Although the Print Server role service does not depend directly on the File Server role service, when you install the Print Server role service, a dependency is exposed when you add a shared print device to the server. Both the Print Services and File Services roles share common RPC and NetBIOS over TCP/IP (NetBT) mechanisms to gain access to shared resources, whether the resources are printers or folders and files. When you first share a printer, you will notice that the File Server role service is automatically enabled, and that you can manage it in Server Manager.

  Firewall rules are predefined and disabled by default for the Print Server role service. The process of installing this role service does not enable these rules. Only installing and sharing a print device enables the rules.

  For more information, see the "Attack Surface" section in this chapter.

- **LPD Service role service**. This role service enables TCP/IP-based printing using the LPD protocol. This role service requires the Printer Server role service to be installed, which minimally expands the attack surface for the Print server. For more information, see the "Attack Surface" section in this chapter.
- **Internet Printing role service**. This role service allows you to make shared printers available to client computers by using the Internet Printing Protocol (IPP) over an HTTP connection. Web browser-based client computers can connect to and use printers that are published using the Web Server role available in Windows Server 2008. Internet printing also enables connections between users and printers that are not on the same domain or network.

  The Internet Printing role service depends on the Web Server (IIS) role, which is installed by Windows Server 2008 automatically when you select the Internet Printing role service. This installation includes a number of Web Server role services and features, including ASP, ISAPI Extensions, ISAPI Filters, .NET Extensibility application development features, Request Filtering, Basic Authentication, Windows Authentication security features, a number of features in the Common HTTP Features role service, the Health and Diagnostics role service, the Performance role service, and the Management Tools role service. Along with these features, the Windows Process Activation Service (WAS) is installed and enabled, which includes configuration application programming interfaces (APIs), and a process model with .NET environment support.

  Because the Internet Printing role service is so dependent on the Web Server role, you should add the attack surface of the Web Server role to the services identified in this section. For more information about the attack surface of the Web Server role, see Chapter 6, "Hardening Web Services" of this guide.

  When you add the Internet Printing role service to a default installation of Windows Server 2008, the installer adds a number of Active Server Pages (ASP) files to the Internet Information Services (IIS) 7.0 server to extend the Web server's functionality to support IPP. No additional services are required for the server, and no additional network ports are opened when you add the Internet Printing role service. This is because the client computer's browser uses the standard Web server ports (80 and 443) to connect to the printer.

  After you install the Internet Printing role service, the print server client computers in your organization can print or manage documents from their Web browsers. When the print server client computers attempt to connect to the printers Web page, the server generates a .cab file that contains the appropriate printer driver files and then downloads the .cab file to the client computers. After the printer drivers install, the printer displays in the Printers folder on the client computer. For more information, see the "Attack Surface" section in this chapter.

The following figure illustrates the role services that make up the Windows Server 2008 Print Server role.

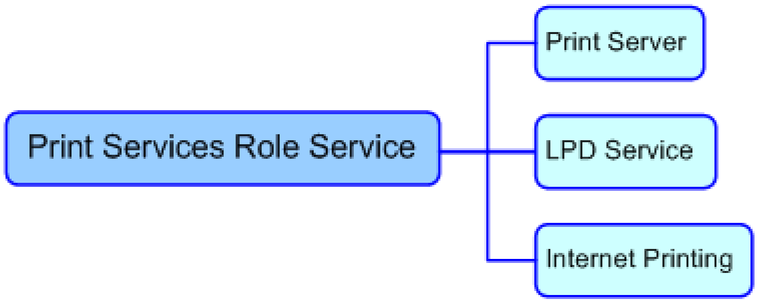


Figure 8.1 Role services hierarchy for the Print Server role

Attack Surface

The Print Services role service allows you to share printers on a network, as well as to centralize print server and network printer management tasks. To determine the attack surface of each service for the Print Server role, you need to identify the following.

- **Installed files**. These are files that are installed as part of each role service for the Print Server role.
- **Installed services**. These are services that are installed as part of each role service for the Print Server role.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. These are the firewall rules that the Print Server role uses.

The details of the attack surface for the Print Server role are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this server role, on the **Print** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Print Server role configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Print Server option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

This section includes configuration recommendations based on best practices to further harden the Print servers in your environment. Recommendations for the LPD Service and Internet Printing role services are not included. For more information about how to configure these services, see Windows Server 2008: Server Management.

The following table summarizes the recommended security configuration tasks for hardening servers performing the Print Server role. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 8.1 Configuration Checklist

	Configuration tasks
	Deploy a server core installation of Windows Server 2008.
	Digitally sign communications.
	Consider Using the Point and Print feature.
	Control printer share access.
	Relocate the default Print Spooler file.

Deploy a Server Core Installation of Windows Server 2008

Deploying Windows Server 2008 using the Server Core installation option further reduces the attack surface of the operating system by reducing the number of installed files and running services. The advantage of the Server Core installation option is that a graphical user interface (GUI) is not installed, so the files and services required by the normal GUI are not installed.

When you use the Server Core installation option of Windows Server 2008 to deploy the operating system, you can only locally manage the server using command-line tools. To manage the server using GUI-based tools, you must install and run these tools on another computer with a Windows-based GUI.

You can use the following command-line management tools to manage the Print Server role:

- To install the Print Server role service, complete the following command:

  ```
  start /w ocsetup Printing-ServerCore-Role
  ```

- To install the Line Printer Daemon (LPD) role service, complete the following command:

  ```
  start /w ocsetup Printing-LPDPrintService
  ```

Note Because the Internet Printing role service depends on .NET Framework features that the Windows Server 2008 Server Core installation does not support, this role service is not available on computers running Server Core installations.

For more information about how to install and manage the Print Server role on a Windows Server 2008 Server Core installation, see *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.

You can also use the following tools to manage your print server:

- Lpg
- Lpr
- Net print
- Print
- Prncnfg.vbs

- Prndrvr.vbs
- Prnjobs.vbs
- Prnmngr.vbs
- Prnport.vbs
- Prnqctl.vbs
- Pubprn.vbs

For information about how to use these tools, see the "Command Reference" section of the Windows Server 2008 TechNet Library.

You can also use WMI scripts or WS-Management and the Windows Remote Shell to remotely manage Print Server role services on computers running Windows Server 2008 Server Core installations.

For more information about WMI, see Windows Management Instrumentation.

For more information about WS-Management and the Windows Remote Shell, see Windows Remote Management.

Note This section assumes that you are running a standard installation of Windows Server 2008. If you have created a Windows Server 2008 Server Core installation for your Print Server role, you can follow these steps using the Microsoft Management Console (MMC) snap-in from a remote computer.

Digitally Sign Communications

The server message block (SMB) protocol provides the basis for Microsoft file and print sharing and many other network operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports SMB packet digital signing. You can configure the Group Policy setting for **Microsoft network server: Digitally sign communications (always)** in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted.

Microsoft recommends to configure the **Microsoft network server: Digitally sign communications (always)** setting to **Enabled** for print servers in both the EC and SSLF environments defined in this guide.

Consider Using the Point and Print Feature

Point and Print is a Windows feature that automatically downloads and installs a printer driver when a user connects to a shared printer. Point and Print also updates the printer driver on the client computer when the driver configuration is updated on the print server. The **Point and Print Restrictions** Group Policy setting has been updated in Windows Server 2008 and Windows Vista to help you manage the improved security of the Point and Print feature.

You can configure the Point and Print group policy settings in the following location in the Group Policy Object Editor:

User Configuration\Administrative Templates\Control Panel\Printers

The following table provides security setting information specific to this technology in Windows Server 2008.

Table 8.2 Point and Print Settings

Policy object	Description	Windows Server 2008 default
Browse the network to find printers	If this setting is enabled or not configured, users can use the Add Printer Wizard to display the list of shared printers on the network. If this setting is disabled, the network printer browse page is removed from the Add Printer Wizard, and users cannot search the network using Windows Explorer.	Not Configured
Only use Package Point and print	If this setting is enabled, users can only point and print to printers that use package-aware drivers. When using package point and print, client computers check the driver signature of all drivers that are downloaded from print servers. If this setting is disabled, or not configured, users are not restricted to package-aware point and print only. This setting only applies to Windows Server 2008 and Windows Vista.	Not Configured
Package Point and print - Approved server	If this setting is enabled, users can only use package point and print to print servers approved by the network administrator. When using package point and print, client computers check the driver signature of all drivers that are downloaded from print servers. If this setting is disabled, or not configured, package point and print is not restricted to specific print servers. This setting only applies to Windows Server 2008 and Windows Vista.	Not Configured

Policy object	Description	Windows Server 2008 default
Point and Print Restrictions	If this policy setting is enabled, client computers are restricted to only point and print to a list of explicitly named servers. When this policy setting is disabled, client computers can point and print to any server. Computers running Windows Vista will *not* display a warning or an elevation prompt when users point and print to a server or when a driver for an existing printer connection needs to be updated.	Not Configured

It is important to understand the options available to you with these Group Policy settings, and how you can use them to maximize the security of client computer printer installations. The option that offers the most security might not work for your environment if you have a wide variety of printers and multifunction print devices that require drivers that Windows Server 2008 does not provide. The following figure shows the options and the tradeoffs for each one.

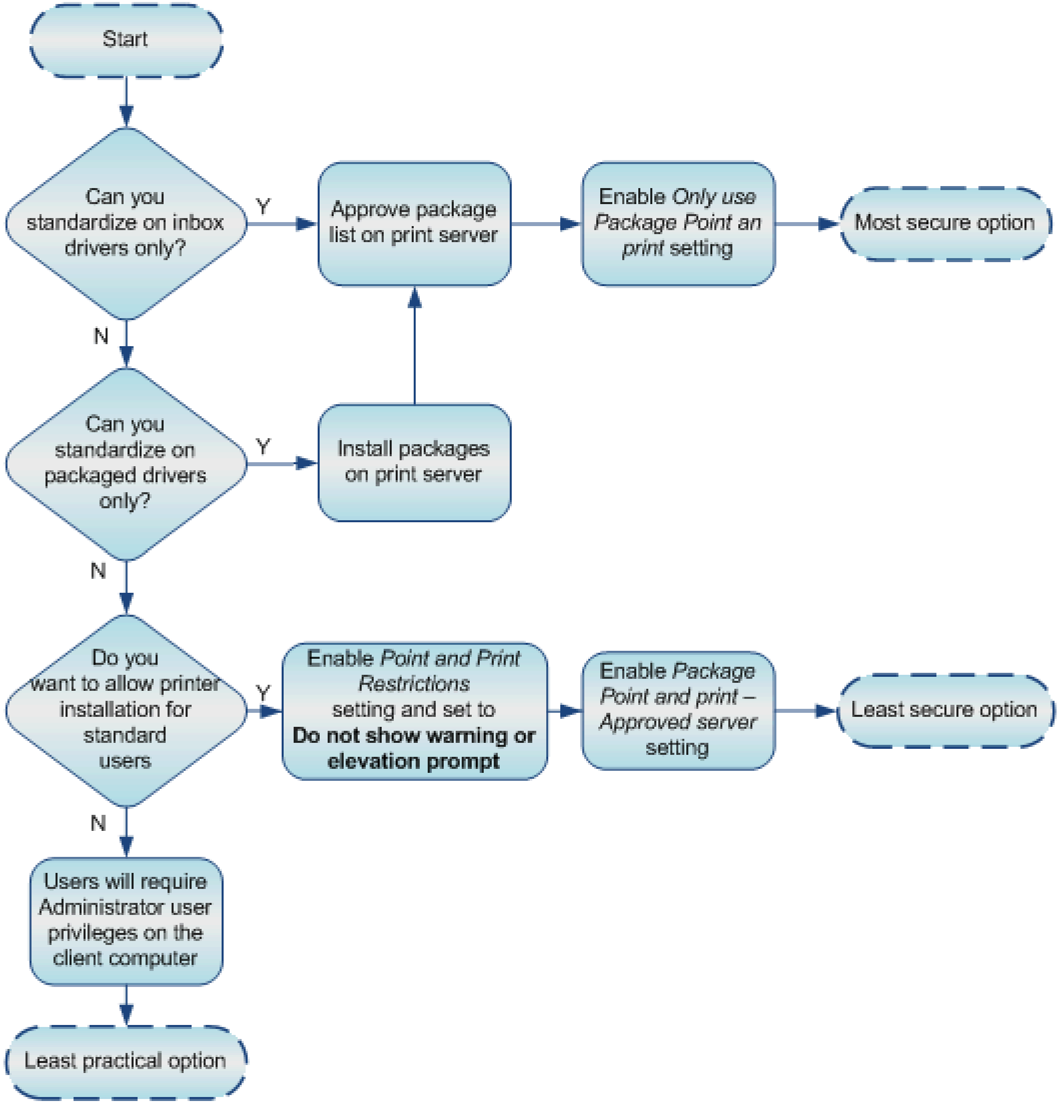

Start
Can you standardize on inbox drivers only?
Y
N
Approve package list on print server
Enable *Only use Package Point an print* setting
Most secure option
Can you standardize on packaged drivers only?
Y
N
Install packages on print server
Do you want to allow printer installation for standard users
Y
N
Enable *Point and Print Restrictions* setting and set to **Do not show warning or elevation prompt**
Enable *Package Point and print – Approved server* setting
Least secure option
Users will require Administrator user privileges on the client computer
Least practical option

Figure 8.2 Secured printing options

The most secure configuration option is to use Group Policy to restrict the printer installations to use only "in-the-box" Windows drivers. These drivers have been through rigorous testing and are signed to ensure that they cannot be tampered with.

However, this option is limiting if your organization already has a wide variety of print devices installed. It is likely that you will need drivers from the printer manufacturers to support your printing requirements. To help support this type of environment, Microsoft has created package point and print drivers. These drivers from printer manufacturers offer the following advantages:

- All driver components are installed on the print client.
- Driver signing and driver integrity are checked on the print client.

- Point and print is more trustworthy and administrators can control it better in a managed environment.

Windows Vista uses package installation as the preferred method of driver installation. However, client computers running earlier versions of Windows® cannot use these drivers because they require a local driver store that was unavailable before Windows Vista. When a client computer running an earlier version of Windows connects to a Windows Server 2008 print server, the print server uses traditional point and print to install the printer on the client computer.

The final option for client computers running Windows Vista is to elevate privileges to allow the installation of print drivers that do not support package point and print. This option requires the user to know the user name and password of a local account that has administrator privileges or requires an administrator to install the printer drivers on behalf of the use. For more information about these options and settings, see the "Point and Print Security in Windows Vista" white paper.

Control Printer Share Access

The default permissions applied to a new printer share on a domain-joined print server are included in the following table.

Table 8.3 Default Printer Permissions

Group or account	Permissions
Everyone	Print
CREATOR OWNER	Manage documents
Administrator	Print, Manage printers, Manage documents

For environments where a raised level of security is required, you can accomplish this by removing permissions from the Everyone group and creating a dedicated user group for the printer. This option increases the overhead for creating and managing access to the printer, but it limits access to the printer to only those users who are specifically granted permissions after you add to them to the dedicated group. Users who are not members of the group are denied access to the printer.

Relocate the Default Print Spooler File

For environments with elevated security or performance requirements, Microsoft recommends to relocate the default print spooler file to a dedicated spooler volume on the Print server.

The following procedure creates a new default spool directory to all printers that are configured on this computer.

To create a new default spool directory

1. Click **Start** and type **Printers**.
2. Open the **Printers** management window.
3. On the **File** menu, click **Server Properties**, and then click the **Advanced** tab.
4. In the **Spool Folder** box, type the path to the dedicated volume, and then click **OK**.

Note For print servers that receive heavy use, monitor the disk performance metrics of the servers to ensure that the print spooler requirements do not overload the server volumes.

More Information

The following resource on Microsoft.com can provide you with further security best practice information about how to design and maintain a server running Windows Server 2008 that performs the Print Server role:

- "Point and Print Security in Windows Vista" white paper.
- *Server Core Installation Option of Windows Server 2008 Step-By-Step Guide*.
- Windows Management Instrumentation.
- Windows Remote Management.
- Windows Server 2008: Server Management.
- Windows Server 2008 TechNet Library.

Chapter 9: Hardening Active Directory Certificate Services

Active Directory® Certificate Services (AD CS) in Windows Server® 2008 provides services that you can customize to create and manage public key certificates in software security systems that employ public key technologies, including version 3 of X.509 certificates. Organizations can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding key pair. AD CS also includes features that allow you to manage certificate enrollment and revocation in a variety of scalable environments.

The role services available for the AD CS role are displayed in the following figure.

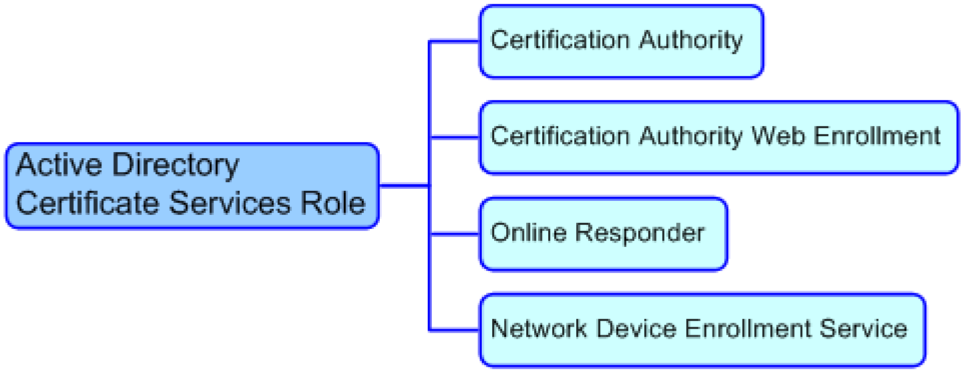

Active Directory Certificate Services Role
Certification Authority
Certification Authority Web Enrollment
Online Responder
Network Device Enrollment Service

Figure 9.1 Role services hierarchy for the AD CS role

This chapter can help you harden server computers that perform the AD CS role. This chapter provides prescriptive guidance for hardening each of the role services available for the AD CS role. Because each AD CS role service has a distinct function, identify those that you want to configure on your server computer, and then use the recommendations in this chapter to harden each role service.

Note The AD CS role service is not available on Server Core installations of Windows Server 2008 or Windows Server 2008 for Itanium-Based Systems.

For more information about the AD CS role service, see Active Directory Certificate Services.

Certification Authority Role Service

The Certification Authority role service allows you to install root and subordinate certification authorities (CAs) to issue certificates to users, computers, and services, and to manage certificate validity.

Requirements to install these CAs include the following:

- To install a root CA, membership in the local Administrators group, or equivalent, is the minimum requirement to complete this procedure. If you are installing an enterprise CA, membership in Domain Admins, or equivalent, is the minimum requirement to complete this procedure. For more information, see "Implement Role-Based Administration" in the Help and Support for Windows Server 2008.
- To install a subordinate CA, membership in the local Administrators group, or equivalent, is the minimum requirement to complete this procedure. If you are installing an enterprise CA, membership in Domain Admins, or equivalent, is the minimum requirement to complete this procedure. For more information, see "Implement Role-Based Administration" in the Help and Support for Windows Server 2008.

Attack Surface

The Certification Authority role service is susceptible to the same security attacks as any CA. To identify the attack surface for this role service, you need to identify the:

- **Installed files**. The files that are installed as part of the Certification Authority role service.
- **Running services**. The services that run as part of the Certification Authority role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the Certification Authority role service uses.
- **Role dependencies**. The dependencies for the Certification Authority role service.

The details of the attack surface for the Certification Authority role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **AD CS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Certification Authority role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Certification Authority role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers performing the Certification Authority role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 9.1 Configuration Checklist

	Configuration tasks
	Deploy an offline root certification authority (CA).
	Protect CAs by using a hardware security module (HSM).
	Deploy an offline policy CA.
	Publish the certificates and CRLs in AD DS.
	Deploy enterprise subordinate CAs.
	Publish both CRLs and delta CRLs.
	Limit the types of certificates that a CA can issue.
	Implement role separation based on Common Criteria specifications.
	Require multifactor authentication for users with PKI management roles.
	Avoid placing policy OIDs and CDP or AIA certificate extensions in root certificates.

Note These recommendations are based on the assumption that your public key infrastructure (PKI) is based on the Rooted Trust Model.

Deploy an Offline Root CA

Although all CAs in a public key infrastructure (PKI) are sensitive, the root CA is the most sensitive because if it is compromised, the entire PKI can be compromised. The root CA is the single point of trust for an entire organization for several organizations.

Important In larger environments, subordinate policy CAs may play the same role as a root CA for different divisions or business units. Deploy these subordinate policy CAs as offline CAs.

To help prevent the root CA from being compromised, Microsoft recommends to take the following security measures:

- **Deploy the root CA as an offline, stand-alone CA.** Deploy the root CA as an offline CA to help prevent network attacks. To deploy an offline root CA, you must deploy the CA as a stand-alone CA because offline enterprise CAs are not supported. For more information about deploying stand-alone CAs, see the following topics in the Help and Support for Windows Server 2008:
  - "Stand-alone Certification Authorities."
  - "Enterprise Certification Authorities."
  - "Install a Root Certification Authority."
- **Protect the computer that is the root CA.** To further protect the root CA, implement one or more of the following security measures:

- **Store the offline CA computers in a physically secure room**. Rather than storing offline CA computers in the standard server room, consider storing the offline CAs in a limited-access server room or in a safe. Allow only those with CA Administration roles to enter the server room or open the safe, and record all attempts to access the server room. Alternatively, you could enforce physical access logs, where any access to the CA computers is logged.
- **Store the CA computers in a secured cage**. Certain models of server cages are available that require PIN codes to open. Some models even track all attempts to access the server cage and allow retrieval of the access logs via serial connections.
- **Store offline CA-related hardware in a separate, secured location**. Some organizations remove the hard disk drives from the CA computers and store them in a remote safe, which requires an attacker to gain access to both the server computer and the hard disk drives before gaining access to an offline CA. This methodology allows companies to use the offline server computer for other uses when the CA is removed from the network.
- **Install the root CA in a virtual environment and store this virtual image in a separate, secured location**. This is a variation of storing offline CA computers in a physically secure room. In this case, the offline CA computer is a virtual image instead of a physical computer.

Protect CAs by Using an HSM

Protect CAs, especially the root CA, using a hardware security module (HSM) with an HSM-operator hardware token to limit access to the CA private key. In addition to limiting access to the CA private key, most HSMs are also hardware cryptographic accelerators that provide better performance than a normal software-based cryptographic system. For more information about HSM, see "Set Up a Certification Authority by Using a Hardware Security Module" in the Help and Support for Windows Server 2008.

Deploy an Offline Policy CA

A policy CA is a type of intermediate CA that is typically used to separate classes of certificates that can be distinguished by policy. For example, policy separation includes the level of assurance that a CA provides or the geographical location of the CA to distinguish different end-entity populations. A policy CA can be online or offline.

Use secure procedures to publish the certificate and CRL of an offline CA. You only need to publish the certificate of the offline CA one time. However, the CRL for the offline CA must be published at regular intervals that correspond to the CRL publication interval value that is configured in the Revoked Certificates Properties of the offline CA.

If the offline CA is maintained in a secure location, such as a data center or vault, it is best if more than one administrator or trusted person publishes the offline CRL within that location, as prescribed in the certificate policy and certificate practice statements for your organization. After the CRL is published, you must transfer it manually from the data center or vault to a location where it can be distributed to your CRL distribution points.

Publish the offline CRL at least several days before the previously issued CRL is set to expire. This allows you to correct any hardware problems or publication failures in advance, ensuring that no interruption in service happens when your offline CRLs are published and replicated to all CRL Distribution Point (CDP) locations.

After the offline CA is installed, configure the various constraint and policy options for certificates that the offline CA issues. These extensions are necessary to ensure that the applications and clients that use the certificates in the hierarchy can perform revocation and chain building as needed.

Microsoft recommends to deploy an offline policy CA by using the same recommendations listed in "Deploying an Offline Root CA" earlier in this chapter. The offline policy CA should be treated similarly to the root CA from a security perspective. However, the policy CA will be brought online more frequently than a root CA.

Publish Certificates and CRLs in AD DS

If your organization uses its PKI to provide certificates for domain users and computers, Microsoft recommends to publish certificates and CRLs in AD DS. AD DS provides a secured repository for certificates and CRLs. By default, the certificates and CRLs are accessed by using Lightweight Directory Access Protocol (LDAP). If the certificates and CRLs cannot be accessed by LDAP, then other methods are attempted if your PKI is configured to publish certificates and CRLs using other publishing methods, such as HTTP.

Both enterprise and stand-alone CAs can publish the certificates and CRLs to Active Directory. By default, enterprise CAs publish certificates and CRLs to the domain in which the CA is a member. You must manually publish certificates and CRLs to other domains and forests. You also must manually configure a stand-alone CA to publish certificates and CRLs in Active Directory.

To install a stand-alone CA so that it will publish its CA certificates and CLR to AD DS, you must be a member of the Domain Admins group of the parent domain in the enterprise, or an administrator with Write access to AD DS. For more information about how to publish a certificate or CRL to Active Directory on a stand-alone CA, see "To publish as certificate or CRL to Active Directory" in Certutil tasks for managing CRLs.

Deploy Enterprise Subordinate CAs

If your organization primarily uses its PKI in your intranet, deploy enterprise subordinate CAs because they automatically publish certificates and CRLs in AD DS. For more information about the advantages of publishing certificates and CRLs in AD DS, see the previous section "Publish Certificates and CRLs in AD DS" in this chapter.

For more information about deploying enterprise subordinate CAs, see the following topics in the Help and Support for Windows Server 2008:

- "Enterprise Certification Authorities."
- "Install a Subordinate Certification Authority."

Publish Both CRLs and Delta CRLs

CRLs can become very long on large CAs that have experienced significant amounts of certificate revocation. This can become a burden for client computers to download frequently. To help minimize frequent downloads of lengthy CRLs, you can publish delta CRLs. This allows client computers to download the most current delta CRL and combine that with the most current base CRL to maintain a complete list of revoked certificates. Because client computers normally store CRLs locally, using delta CRLs can potentially improve performance.

To use delta CRLs, the client application must be aware of and explicitly use delta CRLs for revocation checking. If the client computer does not use delta CRLs, it will retrieve the CRL from the CA every time it refreshes its cache, regardless of whether a delta CRL exists or not. For this reason, ensure to verify that the intended applications use delta CRLs and configure the CA accordingly. If the client computers do not support the use of delta CRLs, either do not configure the CA to publish delta CRLs or configure it so that CRLs and delta CRLs publish at the same interval. This allows new applications that support delta CRLs to use them, while providing current CRLs to all existing applications.

Note All applications that use CryptoAPI in Windows® XP, Windows Vista®, Windows Server® 2003, and Windows Server 2008 use delta CRLs.

Limit the Types of Certificate That a CA Can Issue

Deploy CAs that will issue a specific type of certificate. For example, if you need to issue certificates for smart card authentication or e-mail signing, deploy a CA dedicated to issuing smart card authentication certificates and another CA dedicated to issuing e-mail signing certificates. You can restrict the types of certificates that a CA may issue by using certificate templates. For more information about certificate templates, see Certificate Template Overview.

Implement Role Separation Based on Common Criteria Specifications

Role-based administration is used to organize CA administrators into separate, predefined task-based roles. Microsoft recommends to distribute the management roles among several individuals in your organization to ensure that a single individual cannot compromise PKI services. Role separation enables one person to audit the actions of another person.

Important Limit the number of users that manage your CAs because CAs play a critical security role in a PKI.

Some Common Criteria PKI management roles include the following:

- **PKI Administrator**. Configures and maintains the CA, designates other CA administrators and certificate managers, and renews CA certificates.
- **Certificate Manager**. Approves or denies certificate enrollment requests and revokes issued certificates.
- **Backup Operator**. Performs backups of the CA database, the CA configuration, and the CA’s private and public key pair (also known as a key pair).
- **Audit Manager**. Defines what events are audited for Certificate Services and reviews the security log in Windows Server 2003 for success and failure audit events that are related to Certificate Services.
- **Key Recovery Manager**. Requests retrieval of a private key stored by the service.
- **Enrollee**. Requests certificates from the CA.

For more information about implementing role separation based on Common Criteria specifications, see Defining PKI Management and Delegation.

Require Multifactor Authentication for Users with PKI Management Roles

Human authentication factors are generally classified into the following cases:

- The user knows specific information, such as a password, pass phrase, or personal identification number (PIN).
- The user has a specific device, such as a smart card, security token, software token, phone, or cell phone.
- The user provides a human attribute through an action, such as a fingerprint or retinal pattern, DNA sequence, signature or voice recognition, unique bio-electric signals, or another biometric identifier.

Often organizations use a combination of these methods. For example, a debit card and a PIN, which is also known as *two-factor authentication*.

You can use multifactor authentication to enhance the level of authentication in your organization, compared to only requiring users to provide a password. Multifactor authentication typically includes a physical device, such as a smart card reader, USB security token, or fingerprint reader. Selecting physical devices for multifactor authentication is based on nonsecurity related requirements.

For example, your organization could require smart cards for users that include picture identification, as you can print a picture and a name on the smart card. However, a smart card requires a reader, which may introduce additional costs. A USB token can include flash memory for storing documents and files, and users can plug a USB token into existing USB ports on their computers.

This form of security is recommended for accounts with PKI management roles. Specifically, require multifactor authentication for users who perform the following PKI management roles:

- PKI Administrator
- Certificate Manager
- Backup Operator
- Audit Manager
- Key Recovery Manager

Note If possible, use multifactor authentication throughout the organization to ensure that the strongest possible passwords are required for user accounts. Using multifactor authentication causes the system to automatically generate cryptographically strong random passwords for accounts.

Avoid Placing Policy OIDs and CDP or AIA Certificate Extensions in Root Certificates

As a best practice, Microsoft recommends to avoid placing policy object identifiers (OIDs) in root certificates. By definition, a root CA implements all policies. This applies to both Enterprise and Stand-alone CAs.

At some point in the hierarchy, a CA can have one or more policies defined. When a CA certificate is encountered with any policy OIDs, all certificates below that CA in the hierarchy must also have a subset of those policy OIDs. A certificate chain with no valid policy set will be considered invalid, whereas one with no policy OIDs at all will be considered valid and match the "any policy" OID. This is valid only for Application Policies and not Issuance Polices. For issuance policy, the absence of the certificatePolicies extension in a nonroot certificate implies no issuance policy.

In addition, avoid placing the CRL Distribution Point (CDP) and Authority Information Access (AIA) extensions in root certificates because some applications do not check for root CA revocation.

Relevant Group Policy Settings

There are no Group Policy settings available for the Certification Authority role service.

More Information

The following resources on Microsoft.com provide further security best practice information about how to harden server computers running the Certification Authority role service:

- Active Directory Certificate Services.
- Certutil tasks for managing CRLs.
- Certificate Template Overview.
- Defining PKI Management and Delegation.
- Rooted Trust Model.
- The following Help and Support topics in Windows Server 2008:
  - "Stand-alone Certification Authorities."
  - "Enterprise Certification Authorities."
  - "Install a Root Certification Authority."
  - "Set Up a Certification Authority by Using a Hardware Security Module."
  - "Install a Subordinate Certification Authority."
  - "Implement Role-Based Administration."

Certification Authority Web Enrollment Role Service

The Certification Authority Web Enrollment role service provides an enrollment mechanism for you to issue and renew certificates for the following resources:

- Users and computers that are members of your domain.
- Users and computers that are not joined to your domain.
- Users and computers that are not connected directly to your intranet.
- Users running operating systems other than Windows®.
- Downloading certificate trust lists.

Instead of using the auto-enrollment feature of a CA or the Certificate Request Wizard, you can allow users to request and obtain new and renewed certificates over an Internet or intranet connection by using the Certification Authority Web Enrollment role service.

To install the Certification Authority Web Enrollment role service, membership in Domain Admins, or equivalent, is the minimum requirement to complete this procedure. For more information, see "Implement Role-Based Administration" in the Help and Support for Windows Server 2008.

For more information about the Certification Authority Web Enrollment role service, see AD CS: Web Enrollment.

Role Attack Surface

The Certification Authority Web Enrollment role service is susceptible to the same security attacks as any CA. To identify the attack surface for this role service, you need to identify the:

- **Installed files**. The files that are installed as part of the Certification Authority Web Enrollment role service.
- **Running services**. The services that run as part of the Certification Authority Web Enrollment role service.

Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.

- **Firewall rules**. The Windows Firewall rules that the Certification Authority Web Enrollment role service uses.
- **Role dependencies**. The dependencies for the Certification Authority Web Enrollment role service.

Security Measures

This section describes the security measures that you can incorporate into your Certification Authority Web Enrollment role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Certification Authority Web Enrollment role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers performing the Certification Authority Web Enrollment role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 9.2 Configuration Checklist

	Configuration tasks
	Enable Windows Authentication for intranet-based requests.
	Protect certificate enrollment requests and responses by using Secure Sockets Layer (SSL) encryption.
	Dedicate a computer to the Certification Authority Web Enrollment role service.
	Perform the hardening recommendations for the Web Services (IIS) server role.
	Configure a user account as the designated registration authority.

Enable Windows Authentication for Intranet-Based Requests

When you install the Certificate Web Enrollment role service, the **CertSrv** and **CertEnroll** virtual directories are created in the **Default Web Site**. By default, anonymous authentication is used to access these virtual directories. If the Certificate Web Enrollment role service only services intranet-based computers, you can configure these virtual directories to use Windows Authentication.

Windows authentication uses the NTLM or Kerberos protocols to authenticate client computers. Windows authentication is best suited for an intranet environment. Windows authentication is typically not suited for use over the Internet. Instead use either Basic or Digest authentication for use over the Internet and encrypt all traffic by using SSL.

Important Do not enable anonymous access to the **CertSrv** and **CertEnroll** virtual directories that are created in the **Default Web Site**.

For more information about configuring a Web site to use Windows Authentication, see IIS 7.0: Configuring Authentication in IIS 7.0.

Protect Certificate Enrollment Requests and Responses by Using SSL Encryption

By default, the **CertSrv** and **CertEnroll** virtual directories created in the **Default Web Site** use HTTP. The HTTP protocol sends the certificate enrollment requests and responses in plaintext. Microsoft strongly recommends that you protect this traffic by using SSL encryption.

For more information about how to configure a Web site to protect traffic by using SSL encryption, see "Encrypt data sent between the Web server and client" in the Help and Support for Windows Server 2008.

Dedicate a Computer to the Certification Authority Web Enrollment Role Service

Install the Certification Authority Web Enrollment role service on a computer dedicated to the role service. Although you can install this role service on the same computer that runs the Certification Authority role service, doing so increases the attack surface of the Certification Authority role service.

Installing the Certification Authority Web Enrollment role service on a dedicated computer diverts Web-based traffic from the computer running the Certification Authority role service.

You may want to install the Certification Authority Web Enrollment role service on more than one computer depending on the type of users you are supporting. For example, if you are supporting:

- Users in your intranet, then you may want to install one or more computers running the Certification Authority Web Enrollment role service in your intranet.
- Users on the Internet, then you may want to install one or more computers running the Certification Authority Web Enrollment role service in a perimeter network or extranet in your organization.

Perform the Hardening Recommendations for the Web Services (IIS) Server Role

Because this role service runs on IIS 7.0, ensure to perform the hardening recommendations for the Web Services (IIS) server role. For more information about hardening the Web Services (IIS) Server role, see Chapter 6, "Hardening Web Services" in this guide.

Configure a User Account as the Designated Registration Authority

The Certification Authority Web Enrollment role service needs a set of credentials that it uses to authenticate with the Certification Authority when requesting a certificate, which is known as the designated registration authority.

Microsoft recommends creating a user account to serve as the designated registration authority instead of using the network service account (NetworkService) for this purpose. This is because you can assign only the necessary rights and permissions to a user account, while the NetworkService account may have more rights and permissions than are necessary. In addition, you could affect other software running on the computer if you change the rights and permissions granted to the NetworkService account. The user account must be a member of the Domain and you must add it to the local IIS_IUSRS group.

Relevant Group Policy Settings

There are no Group Policy settings available for the Certification Authority Web Enrollment role service.

More Information

The following resources on Microsoft.com provide further security best practice information about how to harden server computers running the Certificate Authority Web Enrollments role service:

- Active Directory Certificate Services.
- AD CS: Web Enrollment.
- IIS 7.0: Configuring Authentication in IIS 7.0.
- In the Help and Support for Windows Server 2008, see the following topics:
  - "Encrypt data sent between the Web server and client."
  - "Implement Role-Based Administration."

Online Responder Role Service

Certificate revocation is a necessary part of the process of managing the certificates issued by your CAs. The most common means of communicating certificate revocation status is by distributing certificate revocation lists (CRLs). However, in public key infrastructures (PKIs) where the use of conventional CRLs is not an optimal solution, the Online Responder role service can manage and distribute revocation status information by using the Online Certificate Status Protocol (OCSP).

The primary disadvantage of conventional CRLs is their potentially large size, which limits the scalability of the CRL approach. The large size adds significant bandwidth and storage burdens to the CA and relying party, and therefore limits the ability of the system to distribute the CRL. Bandwidth, storage space, and CA processing capacity can also be negatively affected if the publishing frequency gets too high.

Numerous attempts have been made to solve the CRL size issue through the introduction of partitioned CRLs, delta CRLs, and indirect CRLs. All these approaches have added complexity and cost to the system without providing an ideal solution to the underlying problem.

Another drawback of conventional CRLs is latency. Because the CRL publishing period is predefined, information in the CRL might be out of date until a new CRL or delta CRL is published.

Note Microsoft natively supports only CRL and delta CRL in operating systems prior to the Windows Vista operating system. Windows Vista and the Windows Server 2008 will natively support CRL, delta CRL, and OCSP as a method of determining certificate status. The OCSP support includes both the client component as well as the Online Responder, which is the server component.

The Online Responder role service decodes revocation status requests for specific certificates, evaluates the status of these certificates, and then sends back a signed response containing the requested certificate revocation status information.

To install the Online Responder role service, membership in local Administrators, or equivalent, is the minimum requirement to complete this procedure. To configure a CA to support the Online Responder role service, membership in Domain Admins or Enterprise Admins, or equivalent, is the minimum requirement to complete this procedure. For more information about these aspects of administering a PKI, see "Implement Role-Based Administration" in the Help and Support for Windows Server 2008.

For more information about the Online Responder role service, see AD CS: Online Certificate Status Protocol Support.

Attack Surface

The Online Responder role service is susceptible to many of the same security attacks as any server computer that publishes CRLs. To identify the attack surface for this role service, you need to identify the:

- **Installed files**. The files that are installed as a part of the Online Responder role service.
- **Running services**. The services that run as a part of the Online Responder role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the Online Responder role service uses.
- **Role dependencies**. The dependencies for the Online Responder role service.

Security Measures

This section describes the security measures that you can incorporate into your Online Responder role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Online Responder role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers performing the Online Responder role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 9.3 Configuration Checklist

	Configuration tasks
	Enable Windows Authentication for intranet-based requests.
	Protect certificate revocation status requests and responses by using SSL encryption.
	Protect the OCSP signing keys by using an HSM.
	Protect the Online Responder in extranet deployment scenarios.
	Perform the hardening recommendations for the Web Services (IIS) server role.
	Configure a user account as the designated registration authority.

Enable Windows Authentication for Intranet-Based Requests

When you install the Online Responder role service, the **ocsp** virtual directory is created in the **Default Web Site**. By default, anonymous authentication is used to access this virtual directory. When the Online Responder only services intranet-based computers, you can configure the **ocsp** virtual directory to use Windows Authentication.

Windows authentication uses the NTLM or Kerberos protocols to authenticate client computers. Windows authentication is best suited for an intranet environment. Windows authentication is typically not suited for use over the Internet. Instead use either Basic or Digest authentication for use over the Internet and encrypt all traffic by using SSL.

For more information about configuring a Web site to use Windows Authentication, see IIS 7.0: Configuring Authentication in IIS 7.0.

Protect Certificate Revocation Status Requests and Reponses by Using SSL Encryption

By default, the **ocsp** virtual directory created in the **Default Web Site** uses HTTP. The HTTP protocol sends the certificate revocation status requests and responses in plaintext. Microsoft strongly recommends that you protect this traffic by using SSL encryption.

For more information about how to configure a Web site to protect traffic by using SSL encryption, see "Encrypt data sent between the Web server and client" in the Help and Support for Windows Server 2008.

Protect the OCSP Signing Key by Using an HSM

OCSP digitally signs each successful request so that the requestor knows the revocation response came from a legitimate server. The Online Responder role service signs the responses by using an OCSP signing key. The signing key can be obtained from a CA or an HSM.

An HSM can be a plug-in card (PCI) or external device, such as a USB, PCMCIA, SCSI, or RS232 device that generates and stores long term secrets for use in cryptography. An HSM also physically protects access to the secrets. The primary advantage of an HSM is that it provides stronger security for the signing keys that the Online Responder role uses because the HSM is a physical device.

Another advantage is that most HSMs are also hardware cryptographic accelerators. Since the HSMs do not allow the keys to be removed from the device in an unencrypted form, they must be able to perform common cryptographic operations, and they provide better performance than a normal software-based cryptographic system.

For more information about how to configure the Online Responder to use an HSM to protect OCSP signing keys, see "Using an HSM to protect OCSP signing keys" in the *Online Responder Installation, Configuration, and Troubleshooting Guide*.

Protect the Online Responder in Extranet Deployment Scenarios

When you deploy extranet-facing Online Responders, one of the design considerations is to define the level of protection to provide for the Online Responder signing key. The following figure shows two options for protecting the Online Responder.

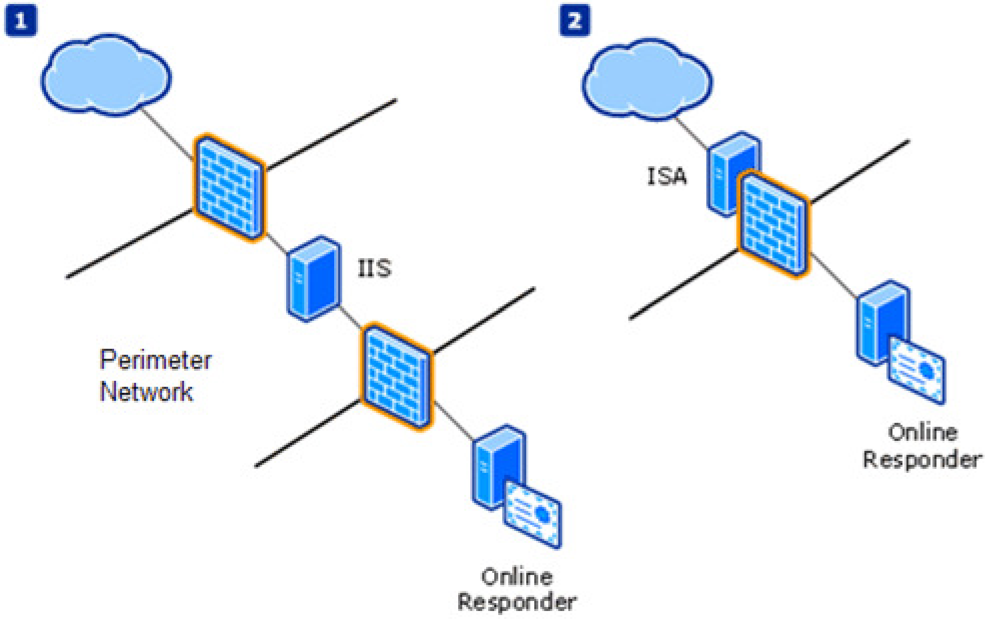


Figure 9.2 Extranet deployment options

In diagram 1 of the previous figure, the Online Responder is located in a protected local area network (LAN), while all requests are redirected by an authenticated server that is running IIS, which is located in a perimeter network (also known as DMZ, demilitarized zone, and screened subnet).

The advantage of such a deployment model is that the firewall configuration requires only pass-through traffic for TCP port 80 for HTTP traffic or TCP port 443 for HTTPS traffic between IIS and the Online Responder. You can achieve similar results by using the reverse-proxy capability of Microsoft Internet Security and Acceleration (ISA) Server as demonstrated in diagram 2 in the previous figure.

For more information about how to protect the Online Responder in extranet deployment scenarios, see "Using an HSM to protect OCSP signing keys" in the *Online Responder Installation, Configuration, and Troubleshooting Guide*.

Perform the Hardening Recommendations for the Web Services (IIS) Server Role

Because this role service runs on IIS 7.0, ensure to perform the hardening recommendations for the Web Services (IIS) server role. For more information about hardening the Web Services (IIS) server role, see Chapter 6, "Hardening Web Services" in this guide.

Configure a User Account as the Designated Registration Authority

The Online Responder role service needs a set of credentials that it uses to authenticate with the Certification Authority when requesting a certificate, which is known as the designated registration authority.

Microsoft recommends to create a user account to serve as the designated registration authority instead of using the network service account (NetworkService) for this purpose. This is because you can assign only the necessary rights and permissions to a user account, while the NetworkService account may have more rights and permissions than are necessary. In addition, you could affect other software running on the computer if you change the rights and permissions granted to the NetworkService account. The user account must be a member of the Domain and you must add it to the local IIS_IUSRS group.

Relevant Group Policy Settings

There are no Group Policy settings available for the Online Responder role service.

More Information

The following resources provide further security best practice information about how to harden server computers running the Online Responder role service:

- Active Directory Certificate Services.
- AD CS: Online Certificate Status Protocol Support.
- IIS 7.0: Configuring Authentication in IIS 7.0.
- *Online Responder Installation, Configuration, and Troubleshooting Guide*.
- "Implement Role-Based Administration" in the Help and Support for Windows Server 2008.

Network Device Enrollment Service Role Service

The Network Device Enrollment Service (NDES) role service allows routers and other network devices that do not have Windows accounts to obtain certificates. NDES is the Microsoft implementation of the Simple Certificate Enrollment Protocol (SCEP), a communication protocol that makes it possible for software running on network devices, such as routers and switches that cannot otherwise be authenticated on the network, to enroll for X.509 certificates from a CA.

To configure the Network Device Enrollment Service role service, membership in the Administrators group is the minimum requirement to complete this procedure. For more information, see "Implement Role-Based Administration" in the Help and Support for Windows Server 2008.

For more information about this role service, see the following resources:

- AD CS: Network Device Enrollment Service.
- Microsoft SCEP Implementation Whitepaper.

Attack Surface

The NDES role service is susceptible to many of the same security attacks as any CA. To identify the attack surface for this role service, you need to identify the:

- **Installed files**. The files that are installed as part of the NDES role service.
- **Running services**. The services that run as part of the NDES role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the NDES role service uses.
- **Role dependencies**. The dependencies for the NDES role service.

Security Measures

This section describes the security measures that you can incorporate into your NDES role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Network Device Enrollment Service role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table summarizes the recommended security configuration tasks for hardening servers performing the NDES role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 9.4 Configuration Checklist

	Configuration tasks
	Configure a user account as the designated registration authority.

	Configuration tasks
	Configure the strongest possible security for the Registration Authority.

Configure a User Account as the Designated Registration Authority

The NDES role service needs a set of credentials that it uses to authenticate with the Certification Authority when requesting a certificate, which is known as the *designated registration authority*.

If you use the NDES role service, Microsoft recommends creating a user account to serve as the designated registration authority instead of using the network service account (NetworkService) for this purpose. This is because you can assign only the necessary rights and permissions to a user account, while the NetworkService account may have more rights and permissions than are necessary. In addition, you could affect other software running on the computer if you change the rights and permissions granted to the NetworkService account. The user account must be a member of the Domain and you must add it to the local IIS_IUSRS group.

For more information about how to configure a user account as the designated registration authority, see "Configure the Network Device Enrollment Service" in the Help and Support for Windows Server 2008.

Configure the Strongest Possible Security for the Registration Authority

The NDES role service uses two certificates and their keys to enable device enrollment. One certificate and key is used to avoid repetition of communication between the CA and the Registration Authority. The other certificate and key are used to secure communication between the Registration Authority and the network device.

Organizations might want to use different Cryptographic Service Providers (CSPs) to store these keys, or they may want to change the length of the keys used by the service. You can specify the configuration for the Registration Authority when you install the NDES role service on the Configure Cryptography for Registration Authority page. Microsoft recommends that you keep the default settings unless you have specific requirements otherwise.

Note Only Cryptographic Application Programming Interface (CryptoAPI) Service Providers are supported for the Registration Authority keys. Cryptography API: Next Generation (CNG) providers are not supported.

Relevant Group Policy Settings

There are no Group Policy settings available for the NDES role service.

More Information

The following resources provide further security best practice information about how to harden server computers running the NDES role service:

- Active Directory Certificate Services.
- AD CS: Network Device Enrollment Service.
- Microsoft SCEP Implementation Whitepaper.

- In the Help and Support for Windows Server 2008, see the following topics:
  - "Implement Role-Based Administration."
  - "Configure the Network Device Enrollment Service."

More Information

The following resources on Microsoft.com provide further security best practice information about how to harden server computers running AD CS role services:

- For the Certification Authority role service, see:
  - Active Directory Certificate Services.
  - Certutil tasks for managing CRLs.
  - Certificate Template.
  - Defining PKI Management and Delegation.
  - Windows Server 2008 Help and Support topics:
    - "Enterprise Certification Authorities."
    - "Install a Root Certification Authority."
    - "Install a Subordinate Certification Authority."
    - "Set Up a Certification Authority by Using a Hardware Security Module."
    - "Stand-alone Certification Authorities."
    - "Implement Role-Based Administration."
- For the Certificate Authority Web Enrollments role service, see:
  - Active Directory Certificate Services.
  - AD CS: Web Enrollment.
  - IIS 7.0: Configuring Authentication in IIS 7.0.
  - Windows Server 2008 Help and Support topics:
    - "Encrypt data sent between the Web server and client."
    - "Implement Role-Based Administration."
- For the Online Responder role service, see:
  - Active Directory Certificate Services.
  - AD CS: Online Certificate Status Protocol Support.
  - IIS 7.0: Configuring Authentication in IIS 7.0.
  - *Online Responder Installation, Configuration, and Troubleshooting Guide*.
  - Windows Server 2008 Help and Support topic:
    - "Implement Role-Based Administration."
- For the Network Device Enrollment Service role service, see:
  - Active Directory Certificate Services.
  - AD CS: Network Device Enrollment Service.
  - Microsoft SCEP Implementation Whitepaper.
  - Windows Server 2008 Help and Support topics:
    - "Configure the Network Device Enrollment Service."

- "Implement Role-Based Administration."

Chapter 10: Hardening Network Policy and Access Services

Network Policy and Access Services (NPAS) in Windows Server® 2008 provides technologies that allow you to deploy and operate a virtual private network (VPN), a dial-up network, 802.1X–protected wired and wireless access, and Cisco Network Admission Control (NAC)–based devices. With NPAS, you can define and enforce policies for network access authentication, authorization, and client health using Network Policy Server (NPS), Routing and Remote Access Service, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).

You can deploy NPS as a Remote Authentication Dial-in User Service (RADIUS) server, RADIUS proxy, both a RADIUS server and proxy, and as a Network Access Protection (NAP) health policy server. NAP helps you ensure that computers connecting to the network are compliant with organization network and client health policies.

Note The NPAS server role is not available on Server Core installations of Windows Server 2008.

This chapter provides prescriptive guidance to help you harden the role services of the NPAS role. The role services within the NPAS role are displayed in the following figure.

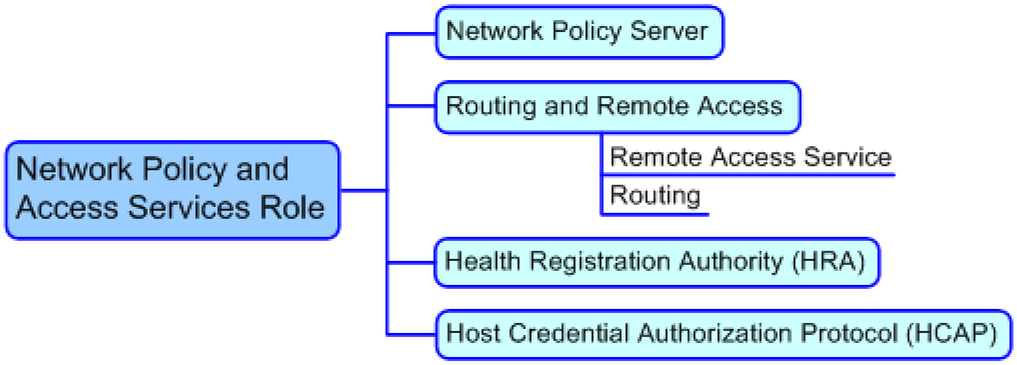

Network Policy and Access Services Role
Network Policy Server
Routing and Remote Access
Remote Access Service
Routing
Health Registration Authority (HRA)
Host Credential Authorization Protocol (HCAP)

Figure 10.1 Role services hierarchy for the NPAS role

Because each of the NPAS role services performs distinct functions, you need to identify the NPAS role services that are configured on your server computer, and then harden each role service.

NPS Role Service

NPS is the Microsoft implementation of a RADIUS server and proxy. You can use NPS to centrally manage network access through a variety of network access servers, including wireless access points, VPN servers, dial-up servers, and 802.1X authenticating switches. In addition, you can use NPS to deploy secure password authentication by using any RFC3748-compliant Extensible Authentication Protocol (EAP) method, such as Protected Extensible Authentication Protocol (PEAP)-MS-CHAP v2 or Lightweight Extensible Authentication Protocol (LEAP). NPS also contains key components for deploying NAP on your network.

For more information about the NPS role service, see the Network Policy Server page on Microsoft® TechNet.

Attack Surface

The NPS role service is susceptible to the same security attacks as any RADIUS server and proxy. To identify the attack surface for this role service, you need to identify the following factors:

- **Installed files**. The files that are installed as part of the NPS role service.
- **Running services**. The services that run as part of the NPS role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the NPS role service uses.
- **Role dependencies**. The dependencies for the NPS role service.

The details of the attack surface for the NPS role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **NPAS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your NPS role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the NPS role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table lists the recommended security configuration tasks for hardening servers performing the NPS role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 10.1 Configuration Checklist

	Configuration tasks
	Restrict traffic based on the services offered.
	Prohibit Legacy RADIUS requests.
	Explicitly specify RADIUS clients.
	Protect computers that run NPS.
	Configure firewall rules on intervening firewalls.

	Configuration tasks
	Use IPsec to secure communication between NPS and RADIUS clients.
	Enable the Message-Authenticator attribute when not using EAP authentication.
	Protect RADIUS shared secrets.
	Use the PEAP or EAP-TLS authentication protocol to authenticate client computers and users.

Restrict Traffic Based On the Services Offered

You can configure the NPS role service to respond to only RADIUS authentication requests, only RADIUS accounting requests, or both by changing the Windows Firewall rules in the following ways:

- On computers that respond to only authentication requests, prohibit the UDP ports that respond to accounting requests (UDP ports 1812 and 1645).
- On computers that respond to only accounting requests, prohibit the UDP ports that respond to authentication requests (UDP ports 1813 and 1646).

Prohibiting unused traffic reduces the attack surface of the computer that runs the NPS role service. For more information about configuring Windows Firewall rules, see "Firewall Rules" in the Windows Server 2008 Help and Support.

Prohibit Legacy RADIUS Requests

The RADIUS protocol standard supports two sets of UDP ports, one pair for the current RADIUS standard (UDP ports 1812 and 1813) and a pair for legacy support (UDP ports 1645 and 1646). When all the NAS devices in your organization support the current RADIUS standard, prohibit the legacy UDP ports by changing the Windows Firewall rules to block inbound traffic to UDP ports 1645 and 1646. For more information about configuring Windows Firewall rules, see "Firewall Rules" in the Windows Server 2008 Help and Support.

Explicitly Specify RADIUS Clients

You can configure NPS to communicate with all RADIUS clients (for example NASs) in your intranet, which is also known as wildcard access. However, this configuration includes all RADIUS clients, including potential rogue RADIUS clients.

To prevent potential rogue RADIUS clients from communicating with NPS, explicitly specify the RADIUS clients to use in your remote access solution. For more information about explicitly specifying a RADIUS client, see "Add a New RADIUS Client" in the Windows Server 2008 Help and Support.

Protect Computers That Run NPS

The server computer that runs the NPS role service needs to communicate with the Active Directory® Domain Services (AD DS) domain controllers to authenticate remote user credentials. Because the NPS server communicates directly with AD DS, place the server computers that run the NPS role service in protected networks, such as your intranet, a secured extranet, or a secured perimeter network. For more information about communication between NPS and domain controllers, see Network Policy Server Infrastructure on TechNet.

Configure Firewall Rules on Intervening Firewalls

RADIUS clients are typically placed in an extranet or perimeter network (also known as DMZ, demilitarized zone, and screened subnet). The computers that run the NPS role service are typically placed in protected networks with one or more firewalls between the RADIUS client and NPS.

Configure the firewall rules on the intermediary firewalls to allow the appropriate kind of traffic. For more information about the types of traffic to allow, see the preceding sections on "Restrict Traffic Based on the Services Offered" and "Prohibit Legacy RADIUS Requests."

Use IPsec to Secure Communication Between NPS and RADIUS Clients

RADIUS clients are typically placed in environments that are less secure than the one in which the computer that runs the NPS role service resides. To prevent potential viewing of the communication between the NPS and RADIUS clients, secure communication by using IPsec, which includes the following protocols:

- **Authentication Header (AH)**. This protocol provides integrity, authentication, and nonrepudiation if the appropriate choice of cryptographic algorithms is made.
- **Encapsulating Security Payload (ESP)**. This protocol provides confidentiality, along with optional authentication and integrity protection that Microsoft strongly recommends.

You can use either of these protocols to secure communication between the NPS and RADIUS clients by using IPsec. However, using both protocols ensures the highest level of protection from IPsec. Microsoft recommends using other IPsec authentication methods instead of preshared keys, such as Kerberos version 5 protocol or public key certificate authentication methods. For more information, see the IPsec overview page on TechNet.

Enable the Message-Authenticator Attribute When Not Using EAP Authentication

When you configure a RADIUS client in NPS, you configure the IP address of the client. If an incoming RADIUS Access-Request message does not originate from at least one of the IP addresses of configured clients, NPS discards the message to protect the NPS server. However, attackers can spoof source IP addresses.

Important Client computers, such as wireless laptop computers and other computers that run client operating systems, are not RADIUS clients. RADIUS clients are network access servers, such as wireless access points, 802.1X authenticating switches, virtual private network (VPN) servers, and dial-up servers. This is because they use the RADIUS protocol to communicate with RADIUS servers, such as Network Policy Server (NPS) servers.

To provide protection from spoofed Access-Request messages and RADIUS message tampering, you can additionally protect each RADIUS message with the **RADIUS Message Authenticator** attribute, which is described in RFC 2869, "RADIUS Extensions." Enabling the **Message Authenticator** attribute provides additional security when PAP, CHAP, MS-CHAP, and MS-CHAP v2 are used for authentication. EAP uses the **Message Authenticator** attribute by default. Therefore, when you use EAP as an authentication method, you do not have to enable the Message Authenticator attribute.

For information about how to configure the **Message Authenticator** attribute for the RADIUS clients of an NPS server, see "Using the Message Authenticator Attribute" in the Windows Server 2008 Help and Support. For information about how to configure the **Message Authenticator** attribute for the Routing and Remote Access service, see "RADIUS Clients" in the Windows Server 2008 Help and Support.

Protect RADIUS Shared Secrets

Shared secrets are used to verify RADIUS messages. With the exception of the Access-Request message, they are sent by a RADIUS-enabled device that is configured with the same shared secret. Shared secrets also verify that the RADIUS message has not been modified in transit to ensure message integrity. The shared secret is also used to encrypt some RADIUS attributes, such as **User-Password** and **Tunnel-Password**. To provide verification for Access-Request messages, you can enable the **RADIUS Message Authenticator** attribute for both the RADIUS client configured on the NPS server and the access server.

Observe the following guidelines and best practices when creating and using a shared secret:

- You must use the same case-sensitive shared secret on both RADIUS devices.
- Use a different shared secret for each RADIUS server-RADIUS client pair.
- To ensure a random shared secret, generate a random sequence at least 22 characters long.
- You can use any standard alphanumeric and special characters.
- You can use a shared secret of up to 128 characters in length. To protect your Microsoft Internet Security and Acceleration (IAS) Server and your RADIUS clients from brute force attacks, use long shared secrets of more than 22 characters.
- Make the shared secret a random sequence of letters, numbers, and punctuation marks and change it often to protect your IAS Server and your RADIUS clients from dictionary attacks. Shared secrets should contain characters from each of the groups listed in the following table:

  Table 10.2 Shared Secret Characters

Group	Examples
Letters (uppercase and lowercase)	A, B, C and a, b, c
Numerals	0, 1, 2, 3
Symbols (all characters not defined as letters or numerals)	Exclamation point (!), asterisk (*), colon (:)

The stronger your shared secret, the more secure the attributes are for such things as passwords and encryption keys that use it. An example of a strong shared secret is 8d#>9fq4bV)H7%a3-zE13sW.

For more information about creating strong shared secrets, see the Shared secrets page on TechNet.

Use the PEAP or EAP-TLS Authentication Protocol to Authenticate Client Computers and Users

Windows®-based operating systems, including Windows Server 2008, support a variety of authentication protocols. The strongest of the supported authentication protocols are Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol - Transport Level Security (EAP-TLS). Both of these authentication protocols provide the security framework for mutual authentication between NPS and client computers.

EAP-TLS is an EAP type of protocol that is used for smart card or certificate-based authentication. EAP-TLS message exchanges provide mutual authentication, integrity-protected cipher suite negotiation, and private key exchange and determination between the access client and the authenticating server. You can use EAP-TLS to authenticate users or computers.

PEAP does not specify an authentication method, but it does provide additional security for other EAP authentication protocols that can operate through the TLS encrypted channel provided by PEAP. PEAP is used as an authentication method for 802.11 wireless client computers, but it is not supported for VPNs or other remote access clients.

You can use PEAP with the following protocols:

- EAP-MS-CHAPv2 (PEAP-EAP-MS-CHAPv2), which is easier to deploy than EAP-TLS because user authentication is accomplished with password-based credentials (user name and password) instead of certificates or smart cards—only the IAS Server or RADIUS server is required to have a certificate.
- EAP-TLS (PEAP-EAP-TLS), which uses certificates for server authentication and either certificates or smart cards for user and client computer authentication. Public Key certificates provide a much stronger authentication method than those that use password-based credentials. To use PEAP-EAP-TLS, you must deploy a public key infrastructure (PKI).

Microsoft recommends using EAP-TLS or PEAP-EAP-TLS to provide the highest possible security for authentication. For more information about the PEAP authentication protocol, see the Protected Extensible Authentication Protocol (PEAP) page on the MSDN® Web site. For more information about EAP-TLS, see the Extensible Authentication Protocol page on TechNet.

Relevant Policy Settings

The following table lists the policy settings that are relevant to the NPS role service. Use these policy settings to enforce the appropriate security configuration in your solution. Configure the policy settings in the following table as a remote access policy on the server computers that run the NPS role service.

Table 10.3 NPS Role Service Remote Access Policy

Policy object	Description
Ignore-User-Dialin-Properties	Ignore any of the dial-in related properties of a user or group account.

More Information

The following resources on Microsoft.com can provide you with additional best practice information about how to harden server computers that run the NPS role service role:

- Extensible Authentication Protocol.
- IPsec overview.
- Network Policy Server.
- Network Policy Server Infrastructure.
- Protected Extensible Authentication Protocol (PEAP).
- "RADIUS Extensions": RFC 2869.
- Server and Domain Isolation.
- Shared secrets.

Routing and Remote Access Role Service

With Routing and Remote Access, you can deploy VPN and dial-up remote access services and multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services. The Routing and Remote Access role service comprises the following subelement role services:

- **Remote Access Service**
- **Routing**

Each subelement role service is discussed in its own respective section.

For more information about the Routing and Remote Access role service, see:

- Routing and Remote Access.
- Routing and Remote Access Blog.

Remote Access Service Role Service

The Remote Access Service role service is a subelement of the Routing and Remote Access role service. The Remote Access Service role service is responsible for providing dial-up and VPN remote access services. Although many of the recommendations presented here are applicable to dial-up remote access services, this guide focuses on hardening server computers that provide VPN remote access services.

Server computers that run this role service are used as NAS devices (RADIUS clients) and should be configured to use the authentication and auditing services provided by NPS. For more information about hardening server computers running the NPS role service, see the "NPS Role Service" section earlier in this chapter.

For more information about the Remote Access Service role service, see:

- Routing and Remote Access.
- Routing and Remote Access Blog.

Attack Surface

The Remote Access Service role service is susceptible to security attacks that are typical of edge-of-network services, but specifically to any VPN services, such as VPN fingerprinting, user name guessing, offline password cracking, man-in-the-middle attacks, and so on. To identify the attack surface for this role service, you need to identify the following factors:

- **Installed files**. The files are installed as part of the Remote Access Service role service.
- **Running services**. The services that run as part of the Remote Access Service role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the Remote Access Service role service uses.

  Note Some of the Windows Firewall rules that the Remote Access Service role service uses are disabled until you run the **Configure and Enable Routing and Remote Access** wizard. For more information about how to run this wizard, see "Install and Enable the Routing and Remote Access Service" in the Windows Server 2008 Help and Support
- **Role dependencies**. The dependencies for the Remote Access Service role service.

The details of the attack surface for the Remote Access Service role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **NPAS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Remote Access Service role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Remote Access Service role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table lists the recommended security configuration tasks for hardening servers that perform the Remote Access Service role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 10.4 Configuration Checklist

	Configuration tasks
	Protect computers that run the Remote Access Service.
	Configure the firewall rules on intermediary firewalls.
	Make computers that run the Remote Access Service members of an extranet forest.
	Use IPsec to secure communication between the Remote Access Service and NPS.

	Configuration tasks
	Protect RADIUS shared secrets.
	Require multifactor authentication for remote users.
	Limit users who can remotely access your intranet.
	Use the PEAP or EAP-TLS authentication protocol to authenticate remote access users and client computers.
	Secure remote access client communication.
	Use NPS to provide centralized user authentication.

Protect Computers That Run the Remote Access Service

The server computer that runs the Remote Access Service role service needs to communicate with remote access client computers through the Internet. Typically, the computers that run the Remote Access Service role service are immediately behind the outward-facing firewalls that provide Internet ingress and egress.

The computers that run the Remote Access Service role service communicate with the computers that run the NPS role service. Because the NPS server communicates directly with AD DS, place the server computers that run the NPS role service in protected networks, such as your intranet, a secured extranet, or a secured perimeter network.

Configure the Firewall Rules on Intermediary Firewalls

The computers that run the Remote Access Service role service are typically placed in your extranet or perimeter network. The computers that run the NPS role service are typically placed in protected networks with one or more firewalls between the computers that run the Remote Access Service and NPS role services.

Configure the firewall rules on the intermediary firewalls to allow the appropriate kind of traffic. For more information about the types of traffic to allow, see the sections "Restrict Traffic Based on the Services Offered" and "Prohibit Legacy RADIUS Requests" earlier in this chapter.

Make Computers that Run the Remote Access Service Members of an Extranet Forest

The computers that run the Remote Access Service role service are typically placed in environments that are less secure than the one in which the computer that runs the NPS role service resides, such as a perimeter network or extranet. Many extranets have an AD DS forest (an extranet forest) that manages the credentials used by services that run on computers in the extranet.

Deploy the computers that run the Remote Access Service role service as members of the extranet forest. The extranet forest typically has a one-way trust with the AD DS forest in your intranet.

Use IPsec to Secure Communication Between the Remote Access Service and NPS

The computers that run the Remote Access Service role service are typically placed in environments that are less secure than the one in which the computer that runs the NPS role service resides. To prevent potential viewing of the communication between the computers that run Routing and Remote Access and NPS, secure communication by using IPsec. For more information about securing communication between Routing and Remote Access and NPS, see the sections "Use IPsec to Secure Communication Between NPS and RADIUS Clients" earlier in this chapter.

Protect RADIUS Shared Secrets

RADIUS shared secrets are used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared secret. The Remote Access Service role service acts as a NAS device (RADIUS client) that communicates with NPS (RADIUS server). For more information about protecting RADIUS shared secrets, see the section "Protect RADIUS Shared Secrets" earlier in this chapter.

Require Multifactor Authentication for Remote Users

Human authentication factors typically belong to one of the following classifications:

- The user knows specific information, such as a password, pass phrase, or personal identification number (PIN).
- The user has a specific device, such as a smart card, security token, software token, phone, or cell phone.
- The user provides a human attribute through an action, such as a fingerprint or retinal pattern, DNA sequence, signature or voice recognition, unique bio-electric signals, or another biometric identifier.

Organizations often use a combination of these methods. An example of such a combination is a debit card and a PIN, which is known as *two-factor authentication*. You can use multifactor authentication to enhance security in your organization, as compared to only requiring users to provide a password. Multifactor authentication typically includes a physical device, such as a smart card reader, USB security token, or fingerprint reader. Selecting physical devices for multifactor authentication is based on requirements that are not related to security.

For example, your organization could require smart cards for users that include picture identification, because you can print a picture and a name on the smart card. However, a smart card requires a reader, which might introduce additional costs. A USB token can include flash memory for storing documents and files, and users can plug a USB token into existing USB ports on their computers.

Microsoft recommends to use two-factor or greater authentication for accounts that have remote access privileges.

Limit Users Who Can Remotely Access Your Intranet

In most remote access scenarios, only a subset of users require remote access. Limit the number of users who can remotely access your intranet based on their individual business needs. As an extra level of precaution, consider the following options:

- **Establish a stringent approval process that requires evaluation of each user request for remote access**. For example, require management approval for remote access requests.
- **Automatically disable remote access after a period of time**. This approach forces re-evaluation of the business requirements for each user's remote access privileges.

Use the PEAP or EAP-TLS Authentication Protocol to Authenticate Remote Access Users and Client Computers

Windows-based operating systems, including Windows Server 2008, support a variety of authentication protocols. The strongest of the supported authentication protocols are Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol – Transport Level Security (EAP-TLS).

EAP-TLS is an EAP type of protocol that is used for smart card or certificate-based authentication. EAP-TLS message exchanges provide mutual authentication, integrity-protected cipher suite negotiation, and private key exchange and determination between the access client and the authenticating server. You can use EAP-TLS to authenticate users or computers.

PEAP does not specify an authentication method, but it does provide additional security for other EAP authentication protocols that can operate through the TLS encrypted channel provided by PEAP. PEAP is used as an authentication method for 802.11 wireless client computers, but it is not supported for VPNs or other remote access clients.

You can use PEAP with the following protocols:

- EAP-MS-CHAPv2 (PEAP-EAP-MS-CHAPv2), which is easier to deploy than EAP-TLS because user authentication is accomplished with password-based credentials (user name and password) instead of certificates or smart cards—only the IAS Server or RADIUS server is required to have a certificate.
- EAP-TLS (PEAP-EAP-TLS), which uses certificates for server authentication and either certificates or smart cards for user and client computer authentication. Public Key certificates provide a much stronger authentication method than those that use password-based credentials. To use PEAP-EAP-TLS, you must deploy a public key infrastructure (PKI).

Microsoft recommends using EAP-TLS or PEAP-EAP-TLS to provide the highest possible security for authentication. For more information about the PEAP authentication protocol, see Protected Extensible Authentication Protocol (PEAP). For more information about EAP-TLS, see Extensible Authentication Protocol.

Secure Remote Access Client Communication

Remote access clients typically connect to computers that run the Remote Access Service role service over the Internet. You need to protect this communication by securing the traffic between the computers that run the Remote Access Service role service and the remote access clients. You can secure this traffic by using either of the following methods:

- **IPsec**. Use the AH and ESP protocols to help secure traffic. For more information, see the IPsec overview page on TechNet.
- **Secure Sockets Tunneling Protocol (SSTP)**. SSTP is a new form of VPN tunnel with features that allow traffic to pass through firewalls that block PPTP and L2TP/IPsec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the SSL channel of the HTTPS protocol. The use of PPP allows support for strong

authentication methods such as EAP-TLS. The use of HTTPS means traffic will flow through TCP port 443, a port commonly used for Web access. Secure Sockets Layer (SSL) provides transport-level security with enhanced key negotiation, encryption, and integrity checking. For more information, see *Step-by-Step Guide: Deploying SSTP Remote Access* on the *Windows Server 2008 Step-by-Step Guides* page of the Microsoft Download Center.

Use NPS to Provide Centralized User Authentication

The Remote Access Service role service can authenticate user accounts that are stored in the following locations:

- **The Local SAM database on the computer that runs the Remote Access Service role service**. This method is not recommended because the local SAM database can be subject to attack if the server is compromised.
- **An AD DS domain of which the computer that runs the Remote Access Service role service is a member**. This method is not recommended because if the server is compromised, the attacker could gain access to the accounts in the domain.
- **An AD DS domain that is connected through a computer that runs the NPS role service**. This method is recommended because there is an extra layer of abstraction between the computer that runs the Remote Access Service role service and the AD DS domain. Authentication of credentials in the AD DS domain can only be performed by the computer that runs the NPS role service. If the computer that runs the Remote Access Service role service is compromised, very little secure information is accessible.

Relevant Group Policy Settings

There are no security-related Group Policy settings for the Remote Access Service role service. However, you can configure NPS (RADIUS) policy settings to help secure users who remotely access your network.

More Information

The following resources on Microsoft.com can provide you with additional best practice information about how to harden server computers that run the Remote Access role service role:

- IPsec overview.
- Routing and Remote Access.
- Routing and Remote Access Blog.
- Server and Domain Isolation.
- *Windows Server 2008 Step-by-Step Guides*: *Step-by-Step Guide: Deploying SSTP Remote Access.*
- Virtual Private Networks.
- Virtual Private Networking with Windows Server 2003: Deploying Remote Access VPNs.

Routing Role Service

The Routing role service is a subelement of the Routing and Remote Access role service. The Routing role service is responsible for providing *edge-of-network routing services*. Typically, these routing services are used to provide point-to-point connections between geographic locations by using dial-up or VPN connections instead of the traditional router within an intranet.

For more information about the Routing role service, see:

- Routing and Remote Access.
- Routing and Remote Access Blog.

Attack Surface

The Routing role service is susceptible to security attacks that are typical of edge-of-network routing services, such as port scanning, transit traffic, receive traffic, man-in-the-middle attacks, and so on. To identify the attack surface for this role service, you need to identify the following factors:

- **Installed files**. The files that are installed as part of the Routing role service.
- **Running services**. The services that run as part of the Routing role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the Routing role service uses.

  Note Some of the Windows Firewall rules that the Routing role service uses are disabled until you run the **Configure and Enable Routing and Remote Access** wizard. For more information on how to run this wizard, see "Install and Enable the Routing and Remote Access Service" in the Windows Server 2008 Help and Support.
- **Role dependencies**. The dependencies for the Routing role service.

The details of the attack surface for the Routing role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **NPAS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Routing role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Routing role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table lists the recommended security configuration tasks for hardening servers that perform the Routing role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 10.5 Configuration Checklist

	Configuration tasks
	Place computers that run the Routing role service in perimeter networks.
	Configure the firewall rules on intervening firewalls.
	Limit routing connections to known end points.
	Make computers that run the Routing role service members of an extranet forest.
	Use secured tunnels to secure communication between routers.
	Require multifactor authentication for authenticating routers.
	Use the PEAP or EAP-TLS authentication protocol to authenticate routers.

Place Computers That Run the Routing Role Service in Perimeter Networks

Typically, the server computer that runs the Routing role service needs to communicate with other computers that run the Routing role service through public networks, such as the Internet. The computers that typically run the Routing role service are immediately behind the outward-facing firewalls that provide Internet ingress and egress.

The computers that run the Routing role service also communicate with others that use it in an intranet. The connection to the intranet is usually sent through the inner-facing firewalls that provide intranet ingress and egress.

Configure the Firewall Rules on Intervening Firewalls

The computers that run the Routing role service are typically placed in your extranet or perimeter network. The routers communicate with the following resources:

- **Other routers through outward-facing firewalls that provide Intranet ingress and egress**. For these firewalls, you need to enable the appropriate ports for one of the following tunneling protocols:
  - **Point-to-Point Tunneling Protocol (PPTP)**. This protocol uses TCP port 1723 and the GRE protocol (protocol ID 47).
  - **Layer 2 Tunneling Protocol (L2TP)**. This protocol uses UDP port 1701 for L2TP, UDP port 500 for Internet Key Exchange (IKE) in IPsec, and UDP 4500 for IPsec Network Address Translation (NAT-T).
  - **SSTP**. This protocol uses TCP port 443 for secured SSL tunneling.
  - **IPsec tunnel mode**. This protocol uses UDP port 500 for IKE in IPsec, and UDP 4500 for IPsec NAT-T.

- **An intranet through inner facing firewalls that provide intranet ingress and egress**. For these firewalls, you need to enable all the protocols that you wish to use between locations. Alternatively, you could connect the router network interface used for intranet communication directly to the intranet instead of connecting the interface to inner-facing firewalls.

Limit Routing Connections to Known End Points

In typical scenarios for the Routing role service, the routing occurs as point-to-point routes between locations in an organization. In such scenarios, the end points of the point-to-point routes are well-defined and limited to a finite number of end points. Ensure that you configure the Routing role service and the outward-facing firewalls to only allow traffic between the end points of the point-to-point routes.

Make Computers That Run the Routing Role Service Members of an Extranet Forest

The computers that run the Routing role service are typically placed in less secure environments, such as a perimeter network or extranet. Many extranets have an AD DS extranet forest that manages the credentials used by services that run on computers in the extranet. These credentials include user accounts and certificates that are used in authenticating router tunnels.

Deploy the computers that run the Routing role service as members of the extranet forest. The extranet forest typically has a one-way trust with the AD DS forest in your intranet.

Use Secured Tunnels to Secure Communication Between Routers

The computers that run the Routing role service communicate with other computers that run the Routing role service over the Internet or other public networks. Most organizations deploy the Routing role service to provide secured, point-to-point routing between locations within the organization.

You can secure traffic between routers by using the following protocols:

- **PPTP**. A VPN tunneling protocol based on Point-to-Point Protocol (PPP) that enables IP traffic to be encrypted, and then encapsulated in an IP header to be sent across private or public IP networks. For more information, see the Point-to-Point Tunneling Protocol (PPTP) page on TechNet.
- **L2TP**. A VPN tunneling protocol that, like PPTP, is also based on PPP. L2TP allows traffic to be encrypted, and then sent over any medium that supports point-to-point datagram delivery, such as IP, X.25, frame relay, or asynchronous transfer mode (ATM). The encryption for L2TP is often provided by ESP in IPsec.
- **SSTP**. A new form of VPN tunnel with features that allow traffic to pass through firewalls that block PPTP and L2TP/IPsec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the SSL channel of the HTTPS protocol. Using PPP allows support for strong authentication methods such as EAP-TLS. Using HTTPS makes traffic flow through TCP port 443, a port commonly used for Web access. Secure Sockets Layer (SSL) provides transport-level security with enhanced key negotiation, encryption, and integrity checking. For more information, see *Step-by-Step Guide: Deploying SSTP Remote Access* on the *Windows Server 2008 Step-by-Step Guides* page of the Microsoft Download Center.

- **IPsec tunnel mode**. For routing, the IPsec protocol is commonly used for encryption in conjunction with L2TP. However, IPsec can be used as a tunneling protocol. IPsec in tunnel mode allows IP packets to be encrypted and then encapsulated in an IP header to be sent across private or public networks. For more information, see the IPsec overview page on TechNet.

Each of the methods for securing traffic allow for mutual authentication of routers and encryption of routed packets.

Require Multifactor Authentication for Router Authentication

You can use multifactor authentication to enhance security for routers. Multifactor authentication typically includes a physical device, such as a smart card reader, USB security token, or fingerprint reader. For routers, the most common physical device is a USB security token or PCMCIA card. Without the physical device, the router is unable to initiate the tunnels with other routers within the organization.

Use the PEAP or EAP-TLS Authentication Protocol to Authenticate Routers

Windows-based operating systems, including Windows Server 2008, support a variety of authentication protocols. The strongest of the supported authentication protocols are Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol - Transport Level Security (EAP-TLS).

Both of these authentication protocols provide the security framework for mutual authentication between computers that run the Routing role service. PEAP is not as secure as Transport Level Security (TLS), but PEAP has the advantage of using username/password authentication instead of client certificate authentication.

For more information about the PEAP authentication protocol, see Protected Extensible Authentication Protocol (PEAP) on MSDN. For more information about EAP-TLS, see Extensible Authentication Protocol on TechNet.

Relevant Group Policy Settings

There are no security-related group policy settings for the Routing role service. However, you can configure NPS (RADIUS) policy settings to help secure the authentication used between routers.

More Information

The following resources on Microsoft.com can provide you with additional best practice information about how to harden server computers that run the Routing role service:

- Configuring Firewalls.
- Extensible Authentication Protocol.
- How to configure an L2TP/IPSec connection by using Preshared Key Authentication.
- IPsec overview.
- Point-to-Point Tunneling Protocol (PPTP).
- Protected Extensible Authentication Protocol (PEAP).
- Routing and Remote Access.
- Routing and Remote Access Blog.

- Server and Domain Isolation.
- *Windows Server 2008 Step-by-Step Guides*: *Step-by-Step Guide: Deploying SSTP Remote Access*.
- Virtual Private Networks.
- Virtual Private Networking with Windows Server 2003: Deploying Site-to-Site VPNs.

HRA Role Service

Health Registration Authority (HRA) is a NAP component that issues health certificates to clients that pass the health policy verification that is performed by NPS using the Statement of Health (SoH) protocol (including security policies). HRA is currently used only when the NAP enforcement method is IPsec enforcement.

However, you could extend this capability to issue health certificates for other enforcements in the future. You can use the HRA to enforce specific health requirements before you allow computers to communicate with each other by refusing to issue certificates or by requiring IPsec connections.

In such a configuration, a server computer that runs the HRA role service acts as a *NAP enforcement point*. Other NAP enforcement points include:

- NAP-capable VPN servers.
- NAP-capable DHCP servers.
- Ethernet switches that support the 802.1X authentication protocol or dynamic VLAN assignments.
- Wireless access points that support 802.1X authentication.

For more information about HRA, see HRA Server Role and Health Registration Authority (HRA) on TechNet. For more information about NAP, HRA, and NAP enforcement points, see Network Access Protection.

Attack Surface

The HRA role service is susceptible to security attacks for any ISAPI extension that runs on Internet Information Services (IIS), which is provided by the Web Server (IIS) role. To identify the attack surface for this role service, you need to identify the following factors:

- **Installed files**. The files that are installed as part of the HRA role service.
- **Running services**. The services that run as part of the HRA role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the HRA role service uses.
- **Role dependencies**. The dependencies for the HRA role service.

The details of the attack surface for the HRA role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **NPAS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your HRA role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the HRA role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table lists the recommended security configuration tasks for hardening servers that perform the HRA role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 10.6 Configuration Checklist

	Configuration tasks
	Place the computers that run the HRA role service in an intranet.
	Make computers that run the HRA role service members of an intranet forest.
	Use IPsec to secure HRA role service communication.
	Use SSL encryption to protect HRA client requests and responses.
	Dedicate a computer to run the HRA role service.
	Allow only authenticated users to obtain health certificates.
	Perform the hardening recommendations for the Web Services (IIS) server role.

Place the Computers That Run the HRA Role Service in an Intranet

The server computer that runs the HRA role service obtains health certificates on behalf of NAP clients when they are determined to be compliant with network health requirements. These health certificates authenticate NAP clients for IPsec-protected communications with other NAP clients on an intranet.

In addition, the HRA role service needs to communicate with computers that run the Certification Authority role service and the NPS role service. In a domain environment, the HRA role service also requires a connection to an Active Directory global catalog for authentication of client credentials. Because of these connectivity requirements, Microsoft recommends to place the computer that runs the HRA role service in a protected subnet of your intranet.

Make Computers That Run the HRA Role Service Members of an Intranet Forest

The computers that run the HRA role service are typically placed in secured subnets in your intranet. Although it is possible to deploy the HRA role service on a stand-alone computer, Microsoft recommends to deploy the computers that run the HRA role service as members of a domain in your intranet forest.

Use IPsec to Secure HRA Role Service Communication

The computers that run the HRA role service communicate with computers that run the Certification Authority role service and the NPS role service. To prevent potential viewing of communication between these computers, secure communication by using IPsec. For more information about securing communication by using IPsec, see the IPsec overview page on TechNet.

Use SSL Encryption to Protect HRA Client Requests and Responses

The HRA role service communicates with client computers by using the HTTP or HTTPS protocols. Microsoft recommends to always configure the HRA to use the HTTPS protocol to communicate with client computers. This configuration encrypts the traffic between the HRA role service and client computers. For more information, see the topics "Certificates for SSL encryption" in "Understanding HRA Authentication Requirements" in the Windows Server 2008 Help and Support.

Dedicate a Computer to Run the HRA Role Service

Install the HRA role service on a computer dedicated to the role service, along with any role service dependencies. Although you can install this role service on the same computer that runs other role services, doing so increases the attack surface of the HRA role service. For more information about role and role service dependencies, see "Attack Surface" earlier in this "HRA Role Service" section.

Allow Only Authenticated Users to Obtain Health Certificates

While installing the HRA role service, you can configure the authentication requirements for HRA. You can configure HRA to allow only authenticated members of a domain to obtain health certificates. You can also configure HRA to allow all users, including anonymous users, to obtain health certificates.

When you provide health certificates for computers in your intranet, always require authenticated users. Only allow anonymous users in limited cases when you want to provide such users with access to a portion of your network. For example, you might want to allow visitors to have Internet access as anonymous users while connected to your intranet.

For more information about this topic, see "Understanding HRA Authentication Requirements" in the Windows Server 2008 Help and Support.

Perform the Hardening Recommendations for the Web Services (IIS) Server Role

Because this role service uses IIS 7.0, ensure to perform the hardening recommendations for the Web Services (IIS) server role. For more information about hardening the Web Services (IIS) server role, see Chapter 6, "Hardening Web Services," in this guide.

Relevant Group Policy Settings

There are no security-related Group Policy settings available for the HRA role service.

More Information

The following resources on Microsoft.com can provide you with additional best practice information about how to harden server computers that run the HRA role service:

- "Certificates for SSL encryption" in the "Understanding HRA Authentication Requirements" section of the Windows Server 2008 Help and Support.
- Health Registration Authority (HRA).
- HRA Server Role.
- IPsec overview.
- Network Access Protection.
- Server and Domain Isolation.
- "Understanding HRA Authentication Requirements" in the Windows Server 2008 Help and Support.

HCAP Role Service

The Host Credential Authorization Protocol (HCAP) allows you to integrate your NAP-based solution with Cisco Network Admission Control (NAC)–based solutions. When you deploy HCAP with NPS and NAP, NPS can perform client health evaluation and the authorization of Cisco NAC–enabled network access devices (such as switches, routers, wireless access points, and VPN concentrators).

In this configuration, a server computer that runs the HCAP role service communicates with the Cisco Secure Access Control Server (ACS) that authorizes the NAC–enabled devices. NPS manages the validation of the health state attributes and the assignment of the overall health state of NAC–enabled devices in the interoperability architecture.

For more information about NAP, HCAP, and NAP enforcement points, see Network Access Protection on TechNet. For more information about NAC, see Network Admission Control on the Cisco Web site.

Attack Surface

The HCAP role service is susceptible to security attacks for any ISAPI extension that runs on IIS, which is provided by the Web Server (IIS) role.

To identify the attack surface for this role service, you need to identify the following factors:

- **Installed files**. The files are installed as part of the HCAP role service.
- **Running services**. The services that run as part of the HCAP role service.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The Windows Firewall rules that the HCA role service uses.
- **Role dependencies**. The dependencies for the HCAP role service.

The details of the attack surface for the HCAP role service are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this role service, on the **NPAS** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into the HCAP role service configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the HCAP role service option on the **Select Role Services** page of the Add Roles Wizard. Recommendations for other role services are not included.

Configuration Checklist

The following table lists the recommended security configuration tasks for hardening servers that perform the HRA role service. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 10.7 Configuration Checklist

	Configuration tasks
	Place computers that run the HCAP role service in an intranet.
	Make computers that run the HCAP role service members of an intranet forest.
	Use IPsec to secure HCAP role service communication.
	Use SSL encryption to protect HCAP requests and responses.
	Dedicate a computer to run the HCAP role service.
	Perform the hardening recommendations for the Web Services (IIS) server role.

Place Computers That Run the HCAP Role Service in an Intranet

The server computer that runs the HRA role service obtains health certificates on behalf of the Cisco Secure ACSs when they are determined to be compliant with network health requirements. These health certificates authenticate the Cisco Secure ACSs for IPsec–protected communications with other NAC–enabled devices and NAP clients on an intranet.

In addition, the HCAP role service needs to communicate with computers that run the Certification Authority role service and the NPS role service. In a domain environment, the HCAP role service also requires a connection to an Active Directory global catalog for authentication of client credentials. Because of these connectivity requirements, Microsoft recommends to place the computer that runs the HCAP role service in a protected subnet of your intranet.

Make Computers That Run the HCAP Role Service Members of an Intranet Forest

The computers that run the HCAP role service are typically placed in secured subnets in your intranet. Although it is possible to deploy the HCAP role service on a stand-alone computer, Microsoft recommends to deploy the computers that run the HCAP role service as members of a domain in your intranet forest.

Use IPsec to Secure HCAP Role Service Communication

The computers that run the HCAP role service communicate with computers that run the Certification Authority role service and the NPS role service. To prevent potential viewing of the communication between these computers, Microsoft recommends to secure them by using IPsec. For more information about securing communication by using IPsec, see the IPsec overview page on TechNet.

Use SSL Encryption to Protect HCAP Requests and Responses

The HCAP role service communicates with client computers by using the HTTP or HTTPS protocols. Microsoft recommends to always configure HCAP to use the HTTPS protocol to communicate with client computers. This configuration encrypts the traffic between the HCAP role service and client computers.

For more information, see "Certificates for SSL encryption" in "Understanding HRA Authentication Requirements" in the Windows Server 2008 Help and Support.

Dedicate a Computer to Run the HCAP Role Service

Install the HCAP role service on a computer that is dedicated to the role service (and any role service dependencies). Although you can install this role service on the same computer that runs other role services, doing so increases the attack surface of the HCAP role service. For more information about role and role service dependencies, see "Attack Surface" earlier in this "HCAP Role Service" section.

Perform the Hardening Recommendations for the Web Services (IIS) Server Role

Because this role service uses IIS 7.0, ensure to perform the hardening recommendations for the Web Services (IIS) server role. For more information about hardening the Web Services (IIS) server role, see Chapter 6, "Hardening Web Services" in this guide.

Relevant Group Policy Settings

There are no security-related Group Policy settings available for the HCAP role service.

More Information

The following resources on Microsoft.com can provide you with additional best practice information about how to harden server computers that run the HCAP role service role:

- "Certificates for SSL encryption" in the "Understanding HRA Authentication Requirements" section of the Windows Server 2008 Help and Support.
- Cisco Network in a Portable Document Format (PDF) file.
- IPsec overview.
- Network Access Protection.
- Network Policy Server.
- Server and Domain Isolation.
- "Understanding HRA Authentication Requirements" in the Windows Server 2008 Help and Support.

More Information

The following resources on Microsoft.com provide additional best practice information about how to harden server computers that run NPAS role services:

- For the NPS role service, see:
  - Extensible Authentication.
  - IPsec overview.
  - Network Policy Server.
  - Network Policy Server Infrastructure.
  - Protected Extensible Authentication Protocol (PEAP).
  - "RADIUS Extensions": RFC 2869.
  - Server and Domain Isolation.
  - Shared secrets.
- For the Remote Access Service role service, see:
  - IPsec overview.
  - Routing and Remote Access.
  - Routing and Remote Access Blog.
  - Server and Domain Isolation.
  - Windows Server 2008 Step-by-Step Guides: *Step-by-Step Guide: Deploying SSTP Remote Access*.
  - Virtual Private Networks.
  - Virtual Private Networking with Windows Server 2003: Deploying Remote Access VPNs.
- For the Routing role service, see:
  - Configuring Firewalls.
  - Extensible Authentication Protocol.
  - How to configure an L2TP/IPSec connection by using Preshared Key Authentication.
  - IPsec overview.
  - Point-to-Point Tunneling Protocol (PPTP).
  - Protected Extensible Authentication Protocol (PEAP).
  - Routing and Remote Access.
  - Routing and Remote Access Blog.
  - Server and Domain Isolation.
  - Windows Server 2008 Step-by-Step Guides: *Step-by-Step Guide: Deploying SSTP Remote Access*.
  - Virtual Private Networks.
  - Virtual Private Networking with Windows Server 2003: Deploying Site-to-Site VPNs.
- For the HRA role service, see:
  - "Certificates for SSL encryption" in the "Understanding HRA Authentication Requirements" section of the Windows Server 2008 Help and Support.
  - Health Registration Authority (HRA).

  - HRA Server Role.
  - IPsec overview.
  - Network Access Protection.
  - Server and Domain Isolation.
  - "Understanding HRA Authentication Requirements" in the Windows Server 2008 Help and Support.
- For the HCAP role service, see:
  - "Certificates for SSL encryption" in the "Understanding HRA Authentication Requirements" section of the Windows Server 2008 Help and Support.
  - Cisco Network in a Portable Document Format (PDF) file.
  - IPsec overview.
  - Network Access Protection.
  - Network Policy Server.
  - Server and Domain Isolation.
  - "Understanding HRA Authentication Requirements" in the Windows Server 2008 Help and Support.

Chapter 11: Hardening Terminal Services

Terminal Services in Windows Server® 2008 supports Remote Desktop Protocol (RDP) 6.0 or later. Windows Server 2008 and Windows Vista® also include the Remote Desktop Connection (RDC) 6.0 client and support it.

Note RDC version 6.1 is available for use on Windows Vista Service Pack 1 (SP1) and Windows® XP Professional SP3. For the best user experience, Microsoft recommends to download the installer package from Microsoft to update your RDC clients to the latest version of either operating system.

In addition to the primary Terminal Services server role, Windows Server 2008 includes the following specific role services:

- **TS Licensing**. The Terminal Services Licensing (TS Licensing) role service manages the Terminal Services client access licenses (TS CALS) that are required for devices and users to connect to a terminal server. You can use this role service to install, issue, and monitor the availability of TS CALs.
- **TS Session Broker**. The Terminal Services Session Broker (TS Session Broker) role service supports reconnection to an existing session on a terminal server that is a member of a load-balanced terminal server farm.
- **TS Gateway**. The Terminal Services Gateway (TS Gateway) role service enables authorized remote users to connect to terminal servers and computers with Remote Desktop enabled on an internal corporate or private network over the Internet. Users can connect from any Internet-connected device that can run the RDC client. The TS Gateway role service does not require users to establish a virtual private network (VPN) session. In addition, this role service uses port 443 to transmit RDP traffic over the HTTP Secure Sockets Layer/Transport Layer Security (SSL/TLS) tunnel. You do not need to open additional ports on the firewall to use this role service.

  When you use Server Manager to install the TS Gateway role service, Server Manager also installs and starts the RPC HTTP Proxy server, the Network Policy and Access Services, the Web Server (IIS) role service, and the Windows Process Activation Services.
- **TS Web Access**. The Terminal Services Web Access (TS Web Access) role service allows you to provide access to Terminal Server sessions through a Web interface. Users that you authorize can gain access to terminal servers by using their Web browser. You can configure the Web interface to advertise applications and connections that are available to the user.

Windows Server 2008 also includes the Terminal Services RemoteApp™ (TS RemoteApp) and Terminal Services Easy Print features.

TS RemoteApp allows users to access programs remotely using Terminal Services. The programs appear as if they are running on the user's local computer. TS RemoteApp enables you to provide users with access to a single application over a remote connection, rather than the entire desktop.

The Terminal Services Easy Print feature allows client computers to redirect print sessions to a local printer without the need for an administrator to install any printer drivers on the terminal server. This feature is not a security feature, but it does significantly reduce the risk to the server of a rogue print driver causing a denial-of-service (DoS) attack.

Each role service provides specific functionality to the enterprise and introduces additional elements that can add to the attack surface of the servers performing this role. The following figures illustrates the five role services that you can select as part of the Windows Server 2008 Terminal Services role.

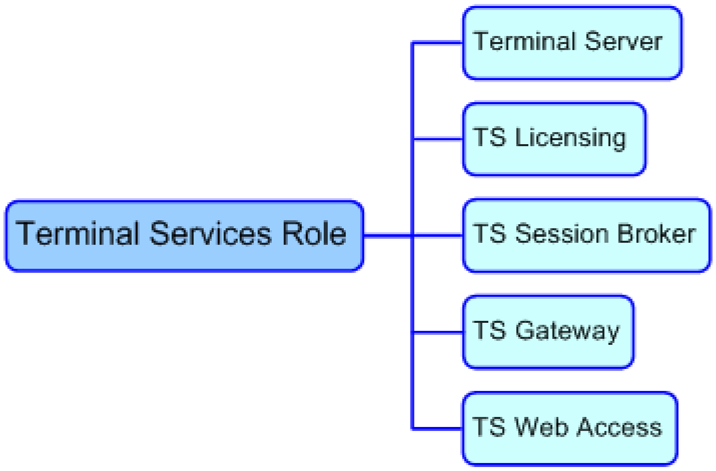


Figure 11.1 Role services hierarchy for Terminal Services

Attack Surface

The Terminal Services server role provides technologies for client computers to access desktop sessions or specific applications running on the terminal server. To determine the attack surface of this server role, you need to identify the following.

- **Installed files**. The files that are installed as part of the Terminal Services server role.
- **Running services**. The services that are installed as part of the Terminal Services server role.

  Note You can use the RootkitRevealer and Sigcheck utilities that are part of Windows Sysinternals to verify the integrity of the installed files and the files that the services run.
- **Firewall rules**. The firewall rules that the Terminal Services server role uses.

The details of the attack surface for the Terminal Services role are included in the Windows Server 2008 Attack Surface Reference workbook that accompanies this Solution Accelerator. To view the attack surface for this server role, on the **Terminal Services** tab of the workbook, view the sections that correspond to each of the items in the previous list.

Security Measures

This section describes the security measures that you can incorporate into your Terminal Services server role configuration to protect the server against malicious attacks. The recommendations that follow assume that you have only selected the Terminal Services option on the **Select Role Services** page of the Add Roles Wizard.

From a security perspective, the Terminal Services role has the greatest attack surface and requires more configuration settings than the other role services that this security guide discusses. However, only the TS Gateway role service has specific configuration changes that relate to security. There are no additional steps to secure the TS Licensing, TS Session Broker, and TS Web Access role services.

Configuration Checklists

There are two main areas to focus on when securing your terminal servers:

- Securing connections to the terminal servers.
- Securing the TS Gateway.

The standard internal network terminal server scenario only requires you to install the Terminal Services server role. This installation adds TCP port 3389 to the server's listening port list, which enables client computers to establish RDP remote desktop sessions with the server. Succeeding sections in this chapter provide more information about each of the recommendations in the following lists.

Securing Connections to the Terminal Servers

The following table summarizes the recommended security configuration tasks for hardening servers performing the Terminal Services role. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 11.1 Terminal Server Configuration Checklist

	Configuration tasks
	Configure the network level authentication.
	Enable Single Sign-On for Terminal Services.
	Enable secure use of saved credentials with Windows Vista RDP clients.
	Change the default RDP port.
	Use smart cards with Terminal Services.
	Use the NTFS file system.
	Use TS Easy Print exclusively.
	Partition user data on a dedicated disk.
	Create specialized OUs for terminal servers.
	Set Group Policy settings for the terminal servers.

	Configuration tasks
	Set Group Policy settings for the remote desktops.
	Restrict users to specific programs.
	Limit terminal server security auditing.

Configure the Network Level Authentication

Network Level Authentication is a new authentication method that completes user authentication before you establish a Remote Desktop connection and the logon screen appears. This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software. Network Level Authentication includes the following advantages:

- It requires fewer server resources initially. The server uses a limited number of resources before authenticating the user, rather than starting a full Remote Desktop connection as in previous versions.
- It can help provide better security by reducing the risk of DoS attacks.

To use Network Level Authentication, you must meet the following requirements:

- The client computer must use Remote Desktop Connection (RDC) 6.0 or later.
- The client computer must run an operating system, such as Windows Vista, that supports Credential Security Support Provider (CredSSP).
- The terminal server must run Windows Server 2008.

You can configure a terminal server to only support connections from client computers running Network Level Authentication. You can set the Network Level Authentication setting for a terminal server in the following ways:

- Use Server Manager to install the Terminal Server role service through the Add Roles Wizard on the **Specify Authentication Method for Terminal Server** page.
- On the **Remote** tab in the **System Properties** dialog box on a terminal server.

  If the **Allow connections from computers running any version of Remote Desktop (less secure)** setting is not selected and is dimmed, the **Require user authentication for remote connections by using Network Level Authentication** Group Policy setting has been enabled and applied to the terminal server.

  To configure the Network Level Authentication setting by using the **Remote** tab in the **System Properties** dialog box on a terminal server, see the "Terminal Services" section of the Windows Server 2008 page of the TechNet Library.
- On the **General** tab of the **Properties** dialog box for a connection in the Terminal Services Configuration tool by selecting the check box for the **Allow connections only from computers running Remote Desktop with Network Level Authentication** setting.

  If the check box for this setting is selected and the setting is dimmed, the Group Policy setting for **Require user authentication for remote connections by using Network Level Authentication** has been enabled and applied to the terminal server.
- By applying the Group Policy setting for **Require user authentication for remote connections by using Network Level Authentication**.

This Group Policy setting is located in **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Security**. You can configure this setting by using either the Local Group Policy Editor or the Group Policy Management Console (GPMC).

Note This Group Policy setting takes precedence over the setting configured in Terminal Services Configuration or on the **Remote** tab.

To determine whether a computer is running a version of RDC that supports Network Level Authentication, start Remote Desktop Connection, click the icon in the upper-left corner of the **Remote Desktop Connection** dialog box, and then click **About**. Look for the phrase "Network Level Authentication supported" in the **About Remote Desktop Connection** dialog box.

For more information about security and Terminal Services, see the Terminal Services page of the Microsoft® TechNet Library.

For more information about Group Policy settings for Terminal Services, see the Terminal Services Technical Reference.

The majority of terminal server users are likely to require the user interface (UI) on the terminal server to be consistent with the UI on their desktop computers. For example, if your users run Windows Vista on their computers, you will need to install the same desktop user experience on the terminal server to provide them with the same UI while running remote desktop sessions.

Enable Single Sign-On for Terminal Services

Single sign-on (SSO) is an authentication method that allows users with a domain account to log on once using a password or smart card, and then gain access to remote servers without being asked for their credentials again.

To implement SSO in Terminal Services, you must meet the following requirements:

- Use can use SSO for remote connections in either of the following scenarios:
  - Support users logging on from a computer running Windows Vista to a terminal server running Windows Server 2008.
  - Support users logging on from one server running Windows Server 2008 to another server running Windows Server 2008.
- User accounts must have appropriate rights to log on to both the terminal server and the client computer running Windows Vista.
- The client computer and terminal server must be joined to a domain.

Configuration Tasks

To configure the recommended settings for your terminal server, complete the following tasks:

- Configure authentication on the terminal server.
- Configure the computer running Windows Vista to allow default credentials to be used for logging on to the specified terminal server.

Membership in the local **Administrators** group, or equivalent, is the minimum requirement to complete this procedure.

To configure authentication on the terminal server

1. Click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration.**
2. Under **Connections**, right-click the appropriate connection (for example, **RDP-Tcp**), and then click **Properties**.
3. On the **General** tab, verify that the **Security Layer** value is set to either **Negotiate** or **SSL (TLS 1.0)**.
4. On the **Log on Settings** tab, ensure that the **Always prompt for password** check box is not selected, and then click **OK.**

To allow default credential usage for single sign-on

1. On the Windows Vista-based computer, click **Start**, and then in the **Start Search** box, type **gpedit.msc** and press ENTER.
2. Expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, and then click **Credentials Delegation.**
3. Double-click **Allow Delegating Default Credentials.**
4. In the **Properties** dialog box, on the **Setting** tab, click **Enabled**, and then click **Show**.
5. In the **Show Contents** dialog box, click **Add.**
6. In the **Add Item** dialog box, in the **Enter the item to be added** box, type **termsrv**/ followed by the name of the terminal server (for example, **termsrv**/**Server1**), click **OK**, and then click **OK** again.

Membership in the local Administrators group, or equivalent, is the minimum requirement to complete this procedure. To review details about using the appropriate accounts and group memberships, see the Why you should not run your computer as an administrator page of the TechNet Library.

For more information about security and Terminal Services, see the Terminal Services page of the TechNet Library.

Enable Secure Use of Saved Credentials with Windows Vista RDP Clients

Windows Vista Credential Delegation policy does not allow a Windows Vista RDP client to send saved credentials to a TS server when the TS server is not authenticated. By default, Windows Vista RDP clients use the Kerberos protocol for server authentication. Alternatively, they can use SSL server certificates, but these are not deployed to servers by default. There are three common scenarios where using the Kerberos protocol to authenticate the server is not possible, but using SSL server certificates is possible. Because SSL server certificates are not deployed by default, using saved credentials does not work when you attempt the following:

- Connect from a home computer to a Terminal Services server through a TS Gateway server.
- Connect to a stand-alone computer.
- Connect to a terminal server farm.

When you connect from home through a TS Gateway server to a terminal server hosted behind a corporate firewall, the TS client has no direct connectivity to a key distribution center hosted on a domain controller behind the corporate firewall. As a result, server authentication using the Kerberos protocol fails. When you connect to a stand-alone server, the Kerberos protocol is not used.

For each of these circumstances, you need to enable server authentication, install SSL certificates issued by a trusted certificate authority (CA), and define the server name in the subject field. Deploy the certificates to all terminal servers that you want to use server authentication. Use the following procedure to add certificates to your terminal servers.

To set the SSL certificate for a connection

1. Click **Start**, click **Run**, and then in the **Open** box type **tsconfig.msc** and click **OK**.
2. In the **Connections** box of the **Configuration for terminal server** pane, double-click **RDP-Tcp**.
3. On the **General** tab, click **Select**.
4. Select the certificate you want to assign to the connection, and click **OK**.

In addition, Kerberos authentication does not work in terminal server farm scenarios because farm names do not have accounts associated with them in Active Directory®. Without these accounts, Kerberos-based server authentication is not possible.

To enable server authentication in a server farm, use SSL certificates that are issued by a trusted CA and that have the farm name in the subject field. Deploy them to all servers in your farm. The SSL certificate will provide server authentication for a terminal server, and the Credential Delegation policy will allow saved credentials to be used for remote connections.

Important A compromised client computer allowed to connect to a TS session could be used to attempt an attack against the Terminal Services server. Microsoft recommends to ensure that all client computers and servers in your organization are adequately protected against malware and are running the latest software updates to help mitigate this risk.

Change the Default RDP Port

If you are concerned about the attack surface exposure of the common RDP port (TCP 3389), you can configure the RDP session to use a different port. However, you must apply the modification to both the terminal server itself and all of the TS clients. It is important to note that changing this port does increase the complexity of both the terminal server deployment and any subsequent audit or troubleshooting steps. For this reason, Microsoft only recommends this step for high risk environments where organizations can justify the overhead required to manage the additional complexity.

For more information about changing the RDP port, see "How to change Terminal Server's listening port": Microsoft Knowledge Base article 187623.

Use Smart Cards with Terminal Services

Terminal Services RDP client sessions in Windows Server 2008 support the ability to authenticate users who log on using smart cards to remote sessions in a domain that uses Active Directory® Domain Service (AD DS). A smart card is a form of *two-factor authentication* that requires the user to have a smart card and know the PIN to gain access to network resources. Smart cards provide secure, tamper-resistant storage for private keys and X.509 security certificates. Smart cards also allow you to require strong credentials from users in a manageable way to provide a more secure environment.

This option provides significant protection against an attacker using a valid user's account credentials to access hosts. If the terminal server requires a valid smart card for a user to log on, an attacker would have to not only know the logon and password details of the user, but also possess the user's smart card. For this reason, Microsoft recommends configuring your terminal server to require smart card authentication if your company has a two-factor authentication policy.

To use smart cards with Windows Server 2008 Terminal Services, you must have AD DS deployed in your organization, and your client computers must run a Microsoft client operating system with built-in smart card support, such as Windows Vista or Windows XP, and most devices that run Windows CE .NET. You must also ensure that the computers users can launch terminal server sessions from smart card readers that are locally installed.

Once you have met these requirements, deploying smart cards for use with Windows Server 2008 Terminal Services is the same as deploying smart cards for use with standard Windows client authentication.

Use the NTFS File System

Microsoft strongly recommends using the NTFS file system as the only file system on terminal server hard disk drives. The file allocation table (FAT) file system does not offer any user and directory security, whereas with NTFS you can limit subdirectories to certain users or groups of users.

This is important in a multi-user system, such as one that uses Terminal Services. Without the security that NTFS provides, any user has access to every directory and file on the terminal server. There also are additional performance advantages available only by using the NTFS file system, such as disk quotas and file system auditing.

Use TS Easy Print Exclusively

TS Easy Print is a new feature in Windows Server 2008 that enables users to reliably print from a TS RemoteApp program or full desktop session to a local or network printer installed on the client computer. Printers can now be supported without the need to install print drivers on the terminal server. When users want to print from a TS RemoteApp program or desktop session, they will see the full printer properties dialog box (printer user interface) from the local client and have access to all the printer functionality.

You can use Group Policy to limit the number of printers redirected to just the default printer, thereby reducing overhead, and improving reliability and scalability. To do this, apply the Group Policy setting for **Redirect only the default client printer**.

This Group Policy setting is located in **Computer Configuration\ Administrative Templates\Windows Components\Terminal Services\Terminal Server\Printer Redirection**.

You can configure this setting by using either the Local Group Policy Editor or the Group Policy Management Console (GPMC). Enabling this policy setting ensures that only the TS client's default printer can be redirected on the TS server. This policy works with connections from any version of the TS client.

Partition User Data On a Dedicated Disk

If you allow users to upload data onto a terminal server's system drive, it is possible the data can seriously affect the server's performance, even to the point of becoming a DoS attack. For this reason, Microsoft recommends storing user data on a dedicated hard disk drive that is isolated from the operating system data.

To do this, you can use the **Terminal Server User Profile** setting in Group Policy to redirect the terminal server user account profile to the user's data drive.

To configure Terminal Services-specific profile settings manually

1. Open Active Directory Users and Computers.
2. Right-click the user account that you want to set profile settings on, and then click **Properties**.
3. Click the **Terminal Services profile** tab.

You can configure the following Terminal Services-specific profile settings manually using the following methods:

- **Terminal Services User Profile path**. You can use this path to choose a place to store users' Terminal Services profiles other than the default location.
- **Terminal Services home folder**. You can specify a path to a home folder for use with Terminal Server sessions. This directory can be either a local folder or a network share.

You also can enforce both of these options directly using Group Policy at the following location:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server

To provide additional protection, consider enabling quota management on the hard disk drive for user data to manage the disk space for users. For more information about using disk quotas, see Working with Quotas in the *Step-by-Step Guide for File Server Resource Manager*.

Create Specialized OUs for Terminal Servers

Where possible, Microsoft recommends that you consider placing the Terminal Server computer objects in a specialized OU to allow you to create system-wide restrictions for your terminal server environment. Doing this enforces computer-based restrictions on the Terminal Server. Administrators have the option to apply user-based restrictions to all users, including administrators who log on to the Terminal Server. You can add these restrictions, or establish them in place of policies for users when they log on to the domain. Refer to the computer loopback policy for additional information.

Note The policies mentioned in this section can severely restrict functionality for even the administrator account.

If you need to apply per-user restrictions, place the user account object into the locked down OU. However, this enforces user-based restrictions for that user account regardless of which computer the user accesses to log on to the domain.

Microsoft recommends one of two approaches when you implement Group Policy for this purpose:

- **Place user accounts into the locked down OU**.

  With this approach, you create Terminal Server-only user accounts and place them in the locked down OU. You can then allow user logons to the Terminal Server for only these users by using the Terminal Server Configuration MMC snap-in. Instruct users to only use these accounts on the Terminal Server. If some computer restrictions are necessary, disable loopback processing and place the Terminal Server computer object in the OU. Aside from the restrictive computer policies, users can have different levels of restrictions on the same Terminal Server. This implementation allows administrators to perform some operations on the Terminal Server while users are active.

- **Place only the Terminal Server computer object in the locked down OU**.

  With this approach, after installing and configuring all applications on the Terminal Server, you can place the Terminal Server computer object in the locked down OU, and then enable loopback processing. All users who log on to the Terminal Server are then restricted by user-based policies defined by the locked down Group Policy object (GPO), regardless of the OU that users are located in.

  This can prevent many local changes from being applied to the Terminal Server. However, an administrator can still remotely maintain the server. If administrators need access to the Terminal Server, log off all users and temporarily restrict their logons to the Terminal Server. Move the Terminal Server computer object out of the locked down OU, then log on. Return the Terminal Server computer object to the locked down OU, and then re-enable user logons after maintenance is complete. This implementation does not require users to have multiple user accounts. It can also prevent configuration changes to the Terminal Server while it is in production.

After you have decided on the policy application approach that you want to use, the next step is to determine the Group Policy settings that you wish to apply to the environment. For the purposes of this guide, recommendations are included for the settings that can be most effective in helping to secure a terminal server installation in the EC and SSLF environments. However, due to potential compatibility and usability issues, these setting are not enforced in the GPOs that the GPOAccelerator tool creates.

Important If you chose to enforce these setting recommendations, it is important to thoroughly test them to determine which ones are most effective in your environment. It is possible that some setting restrictions could cause compatibility issues with some applications that your organization requires.

Set Group Policy Settings for the Terminal Servers

There are a number of Group Policy settings that you can use to configure Terminal Services on a terminal server. This section includes policy object names, descriptions and the purpose of the settings, and recommendations where applicable.

You can use the GPMC to edit policy objects that affect Terminal Services security. The following list represents some of the key areas:

- Security Options
- System Services
- Connections
- Device and Resource Redirection
- Session Time Limits
- Windows Installer
- Group Policy

Security Options Policy Settings

Microsoft recommends using policy settings to control security options in the following location of the GPMC:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.2 Terminal Server Computer Security Options Policy Settings

Policy object	Description	Default
Devices: Restrict CD-ROM access to locally logged-on user only	Recommended setting: Enabled This policy allows only users who log on to the console of the Terminal Server access to the CD-ROM drive. Microsoft recommends to enable this policy to prevent users and administrators from remotely accessing programs or data on a CD-ROM.	Not defined
Devices: Restrict floppy access to locally logged-on user only	Recommended setting: Enabled This policy allows only users who log on to the console of the Terminal Server access to the floppy disk drive. Microsoft recommends to enable this policy to prevent users and administrators from remotely accessing programs or data on a floppy disk.	Not defined

Policy object	Description	Default
Interactive logon: Do not display last user name	Recommended setting: Enabled This policy determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. If this policy is enabled, the name of the last user to successfully log on is not displayed in the **Log On to Windows** dialog box. By default the name of the last user to log on is displayed. Microsoft recommends to enable this setting to hide logon names from users who access the server.	Disabled

System Services Policy Settings

Microsoft recommends to use policy settings to control system services in the following location of the GPMC:

Computer Configuration\Windows Settings\Security Settings\System Services

The following table identifies policy object name, recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.3 Terminal Server Computer System Services Policy Setting

Policy object	Description	Default
Help and Support	Recommended setting: Disabled This policy disables the Help and Support Center service. It prevents users from starting the Windows Help and Support Center application. This policy does not disable help files (such as the *.chm) or Help in other applications. Disabling this service might cause issues with other programs and services that depend on it. Microsoft recommends to disable this service to prevent users from starting other applications or viewing system information about the Terminal Server.	Not defined

Connections Policy Settings

Microsoft recommends using policy settings to control connections in the following location of the GPMC:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Connections

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.4 Terminal Server Computer Connections Policy Settings

Policy object	Description	Default
Restrict Terminal Services users to a single remote session	Recommended setting: Enabled This policy can prevent a single user from creating multiple sessions on the Terminal Server using a single user account.	Not defined
Remove Disconnect option from Shut Down dialog box	Recommended setting: Enabled This policy removes the disconnect option from the **Shut Down Windows** dialog box. It does not prevent users from disconnecting the session to the Terminal Server. Use this policy if you do not want users to easily disconnect from their session and you have not removed the **Shut Down Windows** dialog box.	Not defined

Device and Resource Redirection Policy Settings

Microsoft recommends using policy settings to control resource redirection in the following location of the GPMC:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Device and Resource Redirection

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.5 Terminal Server Computer Device and Resource Redirection Policy Settings

Policy object	Description	Default
Allow audio redirection	Recommended setting: Disabled This policy specifies whether users can choose where to play the remote computer's audio output during a Terminal Services session. Users can use the **Remote computer sound** option on the **Local Resources** tab of Remote Desktop Connection to choose whether to play the remote audio on the remote computer or on the local computer. Users can also choose to disable the audio.	Disabled

Policy object	Description	Default
Do not allow clipboard redirection	Recommended setting: Enabled By default, Terminal Services allows clipboard redirection. This policy specifies whether to prevent the sharing of clipboard contents between a remote computer and a client computer during a Terminal Services session. You can use this setting to prevent users from redirecting clipboard data to and from the remote computer and the local computer.	Not defined
Do not allow COM port redirection	Recommended setting: Enabled By default, Terminal Services allows this COM port redirection. This policy specifies whether to prevent the redirection of data to client COM ports during a Terminal Services session. You can use this setting to prevent users from mapping local COM ports and redirecting data from the remote computer to local COM port peripherals.	Not defined
Do not allow drive redirection	Recommended setting: Enabled By default, Terminal Server maps client hard disk drives automatically upon connection. Microsoft recommends to enable this policy to prevent users from gaining easy access to applications on their local computer via the drive redirection.	Not defined
Do not allow LPT port redirection	Recommended setting: Enabled By default, Terminal Services allows LPT port redirection. This policy specifies whether to prevent the redirection of data to client LPT ports during a Terminal Services session. You can use this setting to prevent users from mapping local LPT ports and redirecting data from the remote computer to local LPT port peripherals.	Not defined
Do not allow supported Plug and Play device redirection.	Recommended setting: Enabled By default, Terminal Services allows redirection of supported Plug and Play devices. Users can use the **More** option on the **Local Resources** tab of Remote Desktop Connection to choose supported Plug and Play devices to redirect then to the remote computer. If you enable this policy, users cannot redirect their supported Plug and Play devices to the remote computer. **Note:** You can also disallow redirection of supported Plug and Play devices on the **Client Settings** tab in	Not defined

Policy object	Description	Default
	the Terminal Services Configuration tool.	
Do not allow smart card device redirection	Recommended setting: Disabled This policy allows you to enable or disable the redirection of smart card devices in a Terminal Services session. Microsoft recommends using smart card devices where possible, and for this reason this setting should not be enabled.	Not defined

Session Time Limits Policy Settings

Microsoft recommends using policy settings to control session time limits in the following location of the GPMC:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Session Time Limits

The following table identifies the policy object name, recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.6 Terminal Server Computer Session Time Limits Policy Setting

Policy object	Description	Default
Set time limit for disconnected sessions	Recommended setting: Enabled By default, Terminal Server allows users to disconnect from a session and keep all of their applications active for an unlimited amount of time. This policy specifies a time limit for disconnected Terminal Server sessions to remain active. Microsoft recommends to enable this policy if you do not want disconnected sessions to remain active for long on the Terminal Server.	Not defined

Windows Installer Policy Settings

Microsoft recommends using policy settings to control Windows® Installer in the following location of the GPMC:

Computer Configuration\Administrative Templates\Windows Components\Windows Installer

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.7 Terminal Server Computer Windows Installer Policy Setting

Policy object	Description	Default
Disable Microsoft Windows Installer	Recommended setting: Enabled If this policy is set for nonmanaged applications only, Windows Installer still functions for applications that are published or assigned by Group Policy. If this policy is set to **Always**, Windows Installer is completely disabled. This may be beneficial if you do not want some published or assigned applications on Terminal Server. Disabling Windows Installer does not prevent application installations from other setup programs or methods. Microsoft recommends installing and configuring applications prior to enabling this policy. After you enable it, administrators cannot install applications that use Windows Installer.	Not defined

User Group Policy Settings

Microsoft recommends using policy settings to control user groups in the following location of the GPMC:

Computer Configuration\Administrative Templates\System\Group Policy

The following table identifies the policy object name, recommended setting and the setting description, and the setting default in Windows Server 2008.

Table 11.8 Terminal Server Computer User Group Policy Setting

Policy object	Description	Default
User Group Policy loopback processing mode	If the Terminal Server computer object is placed in the locked down OU, and the user account is not, loopback processing applies the restrictive user configuration policies to all users on the Terminal Server. If you enable this policy, all users, including administrators who log on to the Terminal Server are affected by the restrictive user configuration policies, regardless of where the user account is located. There are two modes for this policy: • Merge mode first applies to the user's own GPO, then to the locked down policy. The lockdown policy takes precedence over the user's GPO. • Replace mode only uses the locked down	Not defined

Policy object	Description	Default
	policy and not the user's own GPO. This policy enforces restrictions based on computers instead of user accounts. If you disable this policy, and the Terminal Server computer object is placed in the locked down OU, only the computer configuration policies are applied to the Terminal Server. Each user account must be placed into the OU to enforce the user configuration restriction on that user.	

Set Group Policy Settings for the Remote Desktops

When planning the workload configuration for terminal server sessions, there is a number of important steps you can take to optimize the security of sessions for users. Microsoft recommends applying these settings to user accounts that are in the locked down terminal servers OU. If you use loopback processing, all user accounts that log on to computers in the locked down OU also have these restrictions applied.

While many of the settings in this guide work on client computers running Windows Vista SP1 or Windows XP Professional SP3 or later, testing for this guide was only performed on computers running Windows Vista SP1. Ensure to perform your own testing for all of these settings on the client computers that you support in your production environment.

You can use the GPMC to edit policy objects that affect Remote Desktop security. The following list represents some of the key areas:

- Folder Redirection
- Internet Explorer Search
- Internet Explorer Browser Menus
- Application Compatibility
- Internet Explorer
- Common Open File Dialog
- Task Scheduler
- Windows Messenger
- Windows Sidebar
- Windows PowerShell™
- Windows Update
- Start Menu and Taskbar
- Desktop
- Control Panel
- Add or Remove Programs
- Printer
- System
- Ctrl+Alt+Del Options
- Scripts

Folder Redirection Policy Settings

Microsoft recommends using policy settings to control folder redirection in the following location of the GPMC:

User Configuration\Windows Settings\Folder Redirection

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.9 Terminal Server Computer Folder Redirection Policy Settings

Policy object	Description	Default
Application data	Recommended setting: Basic redirection and create a folder for each user under the root path. To do this, on the **Settings** tab, enable the option to grant the user exclusive rights. Enable the option to move the contents of the folder to a new location. Also set the policy removal to redirect the folder back to the local user profile location when the policy is removed.	Not defined
Desktop	Recommended setting: Basic redirection and create a folder for each user under the root path. To do this, on the **Settings** tab, enable the option to grant the user exclusive rights. Enable the option to move the contents of the folder to a new location. Also set the policy removal to redirect the folder back to the local user profile location when the policy is removed.	Not defined
My Documents	Recommended setting: Basic redirection and create a folder for each user under the root path. To do this, on the **Settings** tab, enable the option to grant the user exclusive rights. Enable the option to move the contents of the folder to a new location. Also set the policy removal to redirect the folder back to the local user profile location when policy is removed.	Not defined

Policy object	Description	Default
Start Menu	Recommended setting: Basic redirection and redirect to the following location. To do this, on the **Settings** tab, set the policy removal to redirect the folder back to the local user profile location when the policy is removed. Create a \Programs\Startup folder under this shared folder. Enabling these policies can provide a central point for backing up user data. In addition, if the policy to restrict access to local hard disk drives is enabled, users need folder redirection if they do not want to see messages saying that they have restricted access. If a roaming profile server is not available, you can use local shares. To do this, create a master folder for all of the user data (such as C:\userdata). Create four subfolders, one for each folder type (such as AppData, Desktop, MyDocs, and Start). Share each of the subfolders and then set the share permissions for the Everyone group to Change. Finally, set each path to its corresponding share. You also can configure the Start Menu differently to share it across all users. To do this, change the share permissions from the Everyone group to Read. Ensure to manually create the Programs\Startup folder under the shared Startup folder (C:\userdata\Start\Programs\Startup).	Not defined

Internet Explorer Search Policy Settings

Microsoft recommends using policy settings to control Microsoft Internet Explorer® search behavior in the following location of the GPMC:

User Configuration\Administrative Templates\Windows Components\Internet Explorer

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.10 Terminal Server Computer Internet Explorer Search Policy Setting

Policy object	Description	Default
Search: Disable Find Files via F3 within the browser	Recommended setting: Enabled This policy disables the use of the F3 key to search in Internet Explorer and Windows Explorer. Users cannot press F3 to search the Internet (from Internet Explorer) or to search the hard disk drive (from Windows Explorer). If the user presses F3, a prompt appears informing	Not defined

Policy object	Description	Default
	the user that this feature is disabled. Microsoft recommends to enable this policy to prevent users from searching for applications on their hard disk drives or browsing the Internet.	

Internet Explorer Browser Menus Policy Settings

Microsoft recommends using policy settings to control Internet Explorer browser menus in the following location of the GPMC:

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser menus

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.11 Internet Explorer Menus Policy Settings

Policy object	Description	Default
Disable Context menu	Recommended setting: Enabled This policy prevents the shortcut menu from appearing when users click the right mouse button while using the browser. Microsoft recommends to enable this policy to prevent use of the shortcut menu as an alternate method of running commands.	Not defined
Hide Favorites menu	Recommended setting: Enabled This policy prevents users from adding, removing, or editing the list of Favorites links. If you enable this policy, the Favorites menu is removed from the interface and the Favorites button on the browser toolbar appears dimmed. Use this policy if you want to remove the Favorites menu from Windows Explorer and you do not want to give users easy access to Internet Explorer.	Not defined

For additional Internet Explorer 7.0 security settings that you can use to provide additional restrictions on the browser, see the *Windows Vista Security Guide*.

Application Compatibility Policy Settings

Microsoft recommends using a policy setting to control 16-bit application execution in the following location in the GPMC:

User Configuration\Administrative Templates\Windows Components\Application Compatibility

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.12 Application Compatibility Policy Setting

Policy object	Description	Default
Prevent access to 16-bit applications	Recommended setting: Enabled This policy prevents the MS-DOS® subsystem (ntvdm.exe) from running for the user. This setting affects the start of all 16-bit applications in the operating system. By default, the MS-DOS subsystem runs for all users. Many MS-DOS applications are not Terminal Server friendly and can cause high CPU utilization due to constant polling of the keyboard. Microsoft recommends to enable this policy with the Computer Configuration (system-wide) to block 16-bit applications on the entire terminal server.	Not defined

Internet Explorer Policy Settings

Microsoft recommends using policy settings to control Windows Explorer in the following location in the GPMC:

User Configuration\Administrative Templates\Windows Components\Windows Explorer

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.13 Windows Explorer Policy Settings

Policy object	Description	Default
Remove the Folder Options menu item from the Tools menu	Recommended setting: Enabled This policy removes the Folder Options item from all Windows Explorer menus and removes the Folder Options item from Control Panel. As a result, users cannot use the Folder Options dialog box. Microsoft recommends to enable this policy to prevent users from configuring many properties of Windows Explorer, such as Active Desktop®, Web view, Offline Files, hidden system files, and file types.	Not defined

Policy object	Description	Default
Remove File menu from Windows Explorer	Recommended setting: Enabled This policy removes the File menu from My Computer and Windows Explorer. It does not prevent users from using other methods to perform tasks available on the File menu. Microsoft recommends to enable this policy to remove easy access to tasks such as "New," and "Open With," as well as shell extensions for some applications. Enabling this policy also prevents easy creation of shortcuts to executables.	Not defined
Remove "Map Network Drive" and "Disconnect Network Drive"	Recommended setting: Enabled This policy prevents users from connecting and disconnect to shares with Windows Explorer. It does not prevent mapping and disconnecting hard disk drives from other applications or the run command. Microsoft recommends to enable this policy to remove easy access to browsing the domain from Windows Explorer. If mapped drives are necessary, you can map them from a logon script.	Not defined
Remove Search button from Windows Explorer	Recommended setting: Enabled Microsoft recommends to enable this policy to prevent users from searching for applications from Windows Explorer. This policy does not prevent search routines in other applications or the Start Menu.	Not defined
Remove Security Tab	Recommended setting: Enabled This policy removes the **Security** tab from Windows Explorer. Even if users can open the Properties dialog box for file system objects, including folders, files, shortcuts, and drives, they cannot access the **Security** tab. Microsoft recommends to enable this policy to prevent users from changing the security settings or viewing a list of all users who have access to the object.	Not defined
Remove Windows Explorer's default context menu	Recommended setting: Enabled This policy removes the shortcut menu from Windows Explorer. Microsoft recommends to enable this policy to prevent easy access to applications that place hooks into the shortcut menu. This policy does not remove other methods of accessing applications	Not defined

Policy object	Description	Default
	on the shortcut menu, such as using shortcut hotkeys.	
Hides the Manage item on the Windows Explorer context menu	Recommended setting: Enabled This policy removes the **Manage** option from Windows Explorer or My Computer. The **Manage** option opens the Computer Management MMC snap-in (compmgmt.msc). Users can access items like Event Viewer, System Information, and Disk Administrator from Computer Management. This policy does not restrict access to these tasks from other methods, such as Control Panel and the run command. Microsoft recommends to enable this policy to remove easy access to system information about the Terminal Server.	Not defined
Hide these specified drives in My Computer	Recommended setting: Enabled – Restrict A, B, C, and D drives only. This policy only removes the icons from My Computer, Windows Explorer, and the standard file dialog box. It does not prevent users from access to these drives by other means, such as the command prompt. The policy only allows you to hide drives A through D. Microsoft recommends to enable this policy to hide the floppy disk drive, the CD-ROM drive, and the operating system partition. You can configure a partition for public data to be the only drive that users can view. If required, you can use NTFS permissions to restrict access to this partition. **Important** If you are using BitLocker™ Drive Encryption do not attempt to hide the BitLocker boot drive.	Not defined
Prevent access to drives from My Computer	Recommended setting: Enabled – A, B, C, and D drives only. This policy prevents access to drives A through D with My Computer, Windows Explorer, and the standard file dialog box. This policy does not prevent access from programs that do not use the common dialog boxes. Users can still start applications that reside on the restricted drives. Microsoft recommends to enable this policy to restrict file browsing of system partitions.	Not defined

Policy object	Description	Default
Remove Hardware tab	Recommended setting: Enabled This policy removes the **Hardware** tab from **Mouse**, **Keyboard**, and **Sounds and Audio Devices** items in Control Panel. It also removes the **Hardware** tab from the **Properties** dialog box for all local drives, including hard disk drives, floppy disk drives, and CD-ROM drives. Microsoft recommends to enable this policy to prevent users from using the **Hardware** tab to view the device list or device properties.	Not defined
No Computers Near Me in Network Locations	Recommended setting: Enabled Removes computers in the user's workgroup and domain from lists of network resources in Windows Explorer and Network Locations. This policy removes the **Computers Near Me** option and the icons representing nearby computers from **Network Locations**. This setting also removes these icons from the **Map Network Drive** browser. This policy does not prevent users from connecting to computers in their workgroup or domain by other common methods, such as typing the share name in the **Run** dialog box or the **Map Network Drive** dialog box.	Not defined
No Entire Network in Network Locations	Recommended setting: Enabled This policy removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and Network Locations. This setting removes the **Entire Network** option and the icons representing networked computers from **Network Locations** and from the browser associated with the **Map Network Drive** option. This policy does not prevent users from viewing or connecting to computers in their workgroup or domain. It also does not prevent users from connecting to remote computers by other commonly used methods, such as by typing the share name in the **Run** dialog box or the **Map Network Drive** dialog box.	Not defined

Policy object	Description	Default
Turn on Classic Shell	Recommended setting: Enabled This policy stops users from configuring their system to open items by single-clicking. As a result, the user interface looks and operates like the interface for Windows NT® 4.0, and users cannot restore the new features. Enabling this policy also turns off the preview pane, sets the folder options for Windows Explorer to use the classic folders view, and prevents users from changing these options. **Note:** In operating systems earlier than Windows Vista, enabling this policy also disables the Active Desktop and Web view. This setting also takes precedence over the **Enable Active Desktop** setting. If both policies are enabled, Active Desktop is disabled. Microsoft recommends to enable this policy to remove Folder Tasks. You can use some folder tasks, such as the one for the My Music folder to start Internet Explorer.	Not defined

Common Open File Dialog Policy Settings

Microsoft recommends using policy settings to control file dialog boxes in the following location in the GPMC:

User Configuration\Administrative Templates\Windows Components\Windows Explorer\Common Open File Dialog

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.14 Windows Explorer Policy Settings

Policy object	Description	Default
Hide the common dialog places bar	Recommended setting: Enabled This policy removes the **Back** button from the standard **Open** dialog box available to users in Windows® 2000 Professional, which makes this dialog box appears as it did in Windows NT 4.0 or earlier. This policy affects only programs that use the standard **Open** dialog box provided to developers of Windows programs. In Window Vista, this policy applies only to applications that use the Windows XP common dialog box style. This policy does not apply to the new Windows Vista common dialog box style. Also, third-party applications running with Windows 2000 or later certification are required to	Not defined

Policy object	Description	Default
	adhere to this policy setting.	
Items displayed in Places Bar	Recommended setting: Enabled This policy configures the list of items displayed in the **Places Bar** in the Windows **File**/**Open** dialog box. Enabling this policy allows you to specify from 1 to 5 items to display in the **Places Bar**. Microsoft recommends setting specific places for your terminal server clients. The valid items you can display in the **Places Bar** are: 1. Shortcuts to local folders (for example C:\Windows). 2. Shortcuts to remote folders (for example \\server\share). 3. FTP folders. 4. Web folders. 5. Common Shell folders. The list of Common Shell folders that you can specify include: Desktop, Recent Places, Documents, Pictures, Music, Recently Changed, Attachments, and Saved Searches. If you disable or do not configure this policy the default list of items display in the **Places Bar**. In Windows Vista, this policy applies only to applications that use the Windows XP common dialog box style. This policy does not apply to the new Windows Vista common dialog box style.	Not defined

Task Scheduler Policy Settings

Microsoft recommends using policy settings to control Task Scheduler in the following location in the GPMC:

User Configuration\Administrative Templates\Windows Components\Task Scheduler

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.15 Task Scheduler Policy Settings

Policy object	Description	Default
Hide Property Pages	Recommended setting: Enabled This policy prevents users from viewing and changing the properties of an existing task by removing the **Properties** item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in **Detail** view and in the task preview.	Not defined
Prohibit Task Deletion	Recommended setting: Enabled This policy prevents users from deleting tasks from the Scheduled Tasks folder. However, this policy does not prevent administrators from deleting tasks with the AT command, or from a remote computer.	Not defined
Prevent Task Run or End	Recommended setting: Enabled This policy prevents users from starting and stopping tasks.	Not defined
Prohibit New Task Creation	Recommended setting: Enabled This policy removes the **Add Scheduled Task** item that starts the New Task Wizard. Also, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder. This policy does not prevent administrators from creating new tasks with the AT command, or doing so from a remote computer.	Not defined

Windows Messenger Policy Settings

Microsoft recommends using a policy setting to control Windows Messenger in the following location of the GPMC:

User Configuration\Administrative Templates\Windows Components\Windows Messenger

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.16 Windows Messenger Policy Setting

Policy object	Description	Default
Do not allow Windows Messenger to be run	Recommended setting: Enabled This policy prevents users from running Windows Messenger.	Not defined

Windows Sidebar Policy Settings

Microsoft recommends using a policy setting to control Windows Sidebar in the following location of the GPMC:

User Configuration\Administrative Templates\Windows Components\Windows Sidebar

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.17 Windows Sidebar Policy Setting

Policy object	Description	Default
Turn off Windows Sidebar	Recommended setting: Enabled This policy prevents users from running Windows Sidebar.	Not defined

Windows PowerShell Policy Settings

The Windows PowerShell scripting environment has many advantages, but on a Terminal Server remote desktop there are security risks associated with users who can run PowerShell scripts. By default, PowerShell scripts are not allowed to execute. However, the option for this functionality can be enabled. For this reason, Microsoft recommends using Group Policy to disable this option.

Microsoft recommends using a policy setting to control Windows PowerShell in the following location of the GPMC:

User Configuration\Administrative Templates\Windows Components\Windows PowerShell

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.18 Windows PowerShell Policy Setting

Policy object	Description	Default
Turn on Script Execution	Recommended setting: Disabled This policy allows you to configure the script execution policy to control what scripts can run. Microsoft recommends to disable this policy so that users cannot run scripts.	Not defined

Windows Update Policy Settings

Microsoft recommends using a policy setting to control Windows Update in the following location of the GPMC:

User Configuration\Administrative Templates\Windows Components\Windows Update

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.19 Windows Update Policy Setting

Policy object	Description	Default
Remove access to use all Windows Update features	Recommended setting: Enabled This policy removes access to Windows Update. If you enable this policy, all Windows Update features are removed. This includes blocking access to the Microsoft Windows Update Web site from the Windows Update hyperlink on the Start menu, and also on the Tools menu in Internet Explorer. Windows automatic updating is also disabled; users are not notified about critical updates and do not receive critical updates from Windows Update. This policy also prevents Device Manager from automatically installing driver updates from the Windows Update Web site. You can use this policy to prevent changes to the Terminal Server while it is in production. If you disable Windows Update, you should schedule periodic checks to ensure that Windows® has the latest critical updates.	Not defined

Start Menu and Taskbar Policy Settings

Microsoft recommends using policy settings to control Windows Start Menu and Taskbar in the following location of the GPMC:

User Configuration\Administrative Templates\Start Menu and Taskbar

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.20 Start Menu and Taskbar Policy Settings

Policy object	Description	Default
Remove links and access to Windows Update	Recommended setting: Enabled This policy removes links and access to the Windows Update Web site. The Windows Update Web site is only available for administrators. Microsoft recommends to enable this policy to remove easy access to Internet Explorer for users.	Not defined
Remove common program groups from Start Menu	Recommended setting: Enabled This policy removes shortcuts to programs from the all users' profile. Only the Start Menu in the user's profile or the redirected Start Menu is available. Microsoft recommends to enable this policy to remove easy access to built-in applications, such as games, the calculator, and Windows Media® Player.	Not defined
Remove pinned programs list from Start Menu	Recommended setting: Enabled This policy removes the Pinned Programs list from the Start Menu. It also removes the default links to Internet Explorer and Outlook® Express if they are pinned, and it prevents users from pinning any new programs to the Start Menu. The Frequently Used Programs list is not affected.	Not defined
Remove programs on Settings menu	Recommended setting: Enabled This policy removes Control Panel, Printers, and Network Connections from Settings on the Classic Start menu, My Computer and Windows Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running. However, users can still start Control Panel items by using other methods, such as right-clicking the desktop to open **Display Properties** or right-clicking My Computer to open **System Properties**. Microsoft recommends to enable this policy to prevent easy access to viewing or changing system settings.	Not defined

Policy object	Description	Default
Remove Network Connections from Start Menu	Recommended setting: Enabled This policy prevents the Network Connections folder from opening. The policy also removes Network Connections from Settings on the Start Menu. **Network Connections** still appears in Control Panel and in Windows Explorer, but if users try to start it, a message appears explaining that a setting prevents this action. Microsoft recommends to enable this policy to prevent users from creating new connections, such as VPN or dial-up connections.	Not defined
Remove Search link from Start Menu	Recommended setting: Enabled This policy removes the **Search** item from the Start menu and from the context menu that appears when you right-click the Start menu. Also, the system does not respond when users press the Application key (the Windows logo key)+F. In Windows Explorer, the **Search** item still appears on the Standard buttons toolbar, but the system does not respond when the user presses CTRL+F. Also, the **Search** item does not appear in the context menu when you right-click an icon representing a drive or a folder.	Not defined
Remove Drag-and-Drop context menus on the Start Menu	Recommended setting: Enabled This policy prevents users from using the drag-and-drop method to reorder or remove items on the Start menu. This setting does not prevent users from using other methods of customizing the Start menu or performing the tasks available from the shortcut menus. Microsoft recommends to enable this policy to remove shortcut menus from the Start menu, including tasks such as creating a new shortcut.	Not defined
Remove Favorites menu from Start Menu	Recommended setting: Enabled This policy prevents users from adding the Favorites menu to the Start menu or the Classic Start menu. Use this policy if you do not want users to execute Internet Explorer. The Favorites menu does not appear on the Start menu by default, but this policy disables the Favorites link. This setting only affects the Start menu. The Favorites menu still exists in Windows	Not defined

Policy object	Description	Default
	Explorer and Internet Explorer.	
Remove Help menu from Start Menu	Recommended setting: Enabled This policy removes the Help link from the Start menu. Microsoft recommends to enable this policy to prevent users from easily viewing System Information about the Terminal Server.	Not defined
Remove Run menu from Start Menu	Recommended setting: Enabled Enabling this policy removes the Run command from the Start menu, New Task from Task Manager, and blocks users from typing a UNC path, local drive, and local folders into the Internet Explorer Address bar. Also, users with extended keyboards cannot display the **Run** dialog box by pressing Windows+R.	Not defined
Remove Network icon from Start Menu	Recommended setting: Enabled This policy removes the **Network** icon from the Start menu. Microsoft recommends to enable this policy to prevent easy access to browsing the network.	Not defined
Add Logoff to the Start Menu	Recommended setting: Enabled This policy adds the **Log Off** <*user name*> item to the Start menu and prevents users from removing it. This policy affects the Start menu only. It does not affect the **Log Off** item on the **Windows Security** dialog box that appears when you press CTRL+ALT+DEL or CTRL+ALT+END while using a key board connected to a Terminal Server client computer.	Not defined
Remove and prevent access to Shut Down, Restart, Sleep, and Hibernate commands	Recommended setting: Enabled This policy prevents users from performing the following commands from the Start menu or Windows Security screen: Shut Down, Restart, Sleep, and Hibernate. This policy does not prevent users from running programs to shut down Windows. Microsoft recommends to enable this policy to help remove confusion for the users and prevent administrators from shutting down the system while it is in production.	Not defined

Policy object	Description	Default
Prevent changes to Taskbar and Start Menu Settings	Recommended setting: Enabled This policy prevents users from customizing the taskbar and the Start menu. It can simplify the desktop enforcing the configuration set by the administrator. Microsoft recommends to enable this policy to restrict the ability to add other applications to the Start menu by browsing or typing the location of an application.	Not defined
Remove access to the context menus for the taskbar	Recommended setting: Enabled This policy hides the menus that appear when you right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons. Microsoft recommends to enable this policy to prevent potential access to files and applications by starting Windows Explorer or Search.	Not defined
Force classic Start Menu	Recommended setting: Enabled When this policy is enabled, the Start menu displays the classic Start menu that Windows 2000 displays and the following standard desktop icons: **Documents**, **Pictures**, **Music**, **Computer**, and **Network**. When this policy is disabled, the Start menu only displays the latest UI style, which displays the desktop icons on the Start page.	Not defined

Desktop Policy Settings

Microsoft recommends using policy settings to control the Windows Desktop in the following location of the GPMC:

User Configuration\Administrative Templates\Desktop

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.21 Desktop Policy Settings

Policy object	Description	Default
Remove Properties from the Documents icon context menu	Recommended setting: Enabled This policy hides the **Properties** option of the context menu for the **Documents** icon. Microsoft recommends to enable this policy if shortcut menus are not disabled and you do not want users to easily view or edit the location of	Not defined

Policy object	Description	Default
	their Documents folder.	
Remove Properties from the Computer icon context menu	Recommended setting: Enabled This policy hides the **Properties** option when the user right-clicks **My Computer** or clicks **Computer** and then goes to the File menu. Users also cannot use the ALT+ENTER key combination to display this option when **Computer** is selected.	Not defined
Remove Properties from the Recycle Bin context menu	Recommended setting: Enabled This policy removes the **Properties** option from the Recycle Bin context menu. Microsoft recommends to enable this policy if context menus are not disabled and you do not want users to easily view or change Recycle Bin settings.	Not defined
Hide Network Locations icon on desktop	Recommended setting: Enabled This policy only affects the desktop icon. It does not prevent users from connecting to the network or browsing for shared computers on the network with other methods. Microsoft recommends to enable this policy to remove easy access to browsing the network for applications.	Not defined
Hide Internet Explorer icon on the desktop	Recommended setting: Not defined This policy removes the Internet Explorer icon from the desktop and the Quick Launch bar on the taskbar. Microsoft does not recommend to enable this setting as it does not prevent the user from starting Internet Explorer by using other methods.	Not defined
Prohibit User from manually redirecting Profile Folders	Recommended setting: Enabled This policy prevents users from changing the path to their profile folders. By default, a user can change the location of their individual profile folders, such as Documents, Music, and so on by typing a new path in field for this on the **Locations** tab of the folder's **Properties** dialog box. Microsoft recommends to enable this policy to prevent browsing for applications.	Not defined

Policy object	Description	Default
Hide and disable all items on the desktop	Recommended setting: Not defined This policy removes icons, shortcuts, and other default and user-defined items from the desktop, including Recycle Bin, Computer, and Network. Removing icons and shortcuts does not prevent the user from using another method to start the programs or opening the items they represent. Therefore, Microsoft does not recommend to enable this setting. User can still save and open items on the desktop by using the **Common File** dialog box or Windows Explorer. However, the items do not display on the desktop.	Not defined
Remove My Documents icon on the desktop	Recommended setting: Not defined This policy removes most occurrences of the **My Documents** icon. It does not prevent users from applying other methods to gain access to the contents of the My Documents folder. Therefore, Microsoft does not recommend to enable this setting.	Not defined
Remove Computer icon on the desktop	Recommended setting: Enabled This policy hides the **Computer** icon from the desktop and from the new Start menu. It also hides links to Computer in the Web view of all Explorer windows, and it hides Computer in the Explorer folder tree pane. If the user navigates into Computer by using the **Up** icon when this setting is enabled, an empty Computer folder displays. Microsoft recommends to enable this policy to present users with a simpler desktop environment from using this icon, and remove easy access to Computer Management and System Properties by no longer allowing users to right-click the icon.	Not defined

Control Panel Policy Settings

Microsoft recommends using policy settings to restrict Control Panel in the following location of the GPMC:

User Configuration\Administrative Templates\Control Panel

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.22 Control Panel Policy Setting

Policy object	Description	Default
Prohibit access to the Control Panel	Recommended setting: Enabled This policy removes access to Control Panel and disables all Control Panel programs. It also prevents Control.exe, the program file for Control Panel, from starting. Microsoft recommends to enable this setting to prevent users from viewing configuration information about the Terminal Server.	Not defined

Add or Remove Programs Policy Settings

Microsoft recommends using policy settings to control the Add or Remove Programs Control Panel item in the following location of the GPMC:

User Configuration\Administrative Templates\Control Panel\Add or Remove Programs

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.23 Add or Remove Programs Policy Setting

Policy object	Description	Default
Remove Add or Remove Programs	Recommended setting: Enabled This policy removes Add or Remove Programs from Control Panel and removes the **Add or Remove Programs** item from menus. If access to Control Panel is prohibited, you can use this policy to remove the links to Add or Remove Programs from places like Computer. The link then displays an access denied message if a user clicks it. This policy does not prevent users from using other tools and methods to install or uninstall programs. Microsoft recommends to enable this policy to prevent users from viewing Terminal Server configuration information.	Not defined

Printer Policy Settings

Microsoft recommends using policy settings to control the Printers Control Panel item in the following location of the GPMC:

User Configuration\Administrative Templates\Control Panel\Printers

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.24 Printer Policy Setting

Policy object	Description	Default
Prevent addition of printers	Recommended setting: Enabled This policy prevents users from using familiar methods to add local and network printers. This policy does not prevent the autocreation of Terminal Server redirected printers, nor does it prevent users from running other programs to add printers. Microsoft recommends to enable this policy to prevent users from browsing the network or searching Active Directory for printers.	Not defined

For more information about controlling the security of printers, see Chapter 8, "Hardening Print Services" of this guide.

System Policy Settings

Microsoft recommends using policy settings to control the System in the following location of the GPMC:

User Configuration\Administrative Templates\System

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.25 System Policy Settings

Policy object	Description	Default
Prevent access to the command prompt	Recommended setting: Enabled Configure the **Disable the command prompt script processing also** setting to **No**. This policy prevents users from running the interactive command prompt Cmd.exe. From the command prompt users can start applications. This policy also determines whether batch files (.cmd and .bat files) can run on the computer. **Important** Do not prevent the computer from running batch files on a Terminal Server. This policy does not prevent access to Command.com (16-bit command interpreter). To disable Command.com, you can restrict access with NTFS permission, or disable all 16-bit applications with the **Prevent access to 16-bit application** policy setting. Microsoft recommends to enable the **Prevent access to the command prompt** policy setting to prevent users from bypassing other policy settings by using the command prompt instead of Windows Explorer as the shell.	Not defined
Prevent access to registry editing tools	Recommended setting: Enabled This policy blocks user access to Regedit.exe. It does not prevent other applications for editing the registry. Microsoft recommends to enable this policy to prevent users from changing their shell to the command prompt or bypassing other policies.	Not defined

Policy object	Description	Default
Run only specified Windows applications	Recommended setting: Enabled – Define list of authorized applications This policy only prevents users from running programs that Windows Explorer starts. It does not prevent users from running programs such as Task Manager that a user can start with a system process. Also, if users can access the command prompt, Cmd.exe, this setting does not prevent them from starting programs from the command window, which they can access using Windows Explorer. Microsoft recommends to enable this policy to restrict users to only run programs that are added to the List of Allowed Applications.	Not defined

Ctrl+Alt+Del Options Policy Settings

Microsoft recommends using policy settings to control the CTRL+ALT+DEL options in the following location of the GPMC:

User Configuration\Administrative Templates\System\Ctrl+Alt+Del Options

The following table identifies policy object names, recommended settings and setting descriptions, and the setting defaults in Windows Server 2008.

Table 11.26 Ctrl+Alt+Del Options Policy Settings

Policy object	Description	Default
Remove Task Manager	Recommended setting: Enabled This policy prevents users from starting Task Manager. Microsoft recommends to enable this policy to prevent users from using Task Manager to start and stop programs, monitor the performance of the Terminal Server, and search for the executable names of applications.	Not defined
Remove Lock Computer	Recommended setting: Not defined This policy prevents users from locking their sessions. Users can still disconnect and log off. While locked, the desktop cannot be used. Only the user who locked the system or the system administrator can unlock it. Microsoft does not recommend to enable this setting as users may need to lock their session to prevent access to it while they are away from their computer.	Not defined

Scripts Policy Settings

Microsoft recommends using policy settings to control script execution behavior in the following location of the GPMC:

User Configuration\Administrative Templates\System\Scripts

The following table identifies the policy object name, the recommended setting and setting description, and the setting default in Windows Server 2008.

Table 11.27 Script Policy Setting

Policy object	Description	Default
Run legacy logon scripts hidden	Recommended setting: Enabled This policy hides the instructions in logon scripts written for Windows NT 4.0 and earlier. Microsoft recommends to enable this policy to prevent users from viewing or interrupting logon scripts written for Windows NT 4.0 or earlier.	Not defined

Restrict Users to Specific Programs

Software restriction policies provide administrators with a policy-driven mechanism to identify software programs running on computers in a domain and to control the ability of those programs to execute. You can use policies to block malicious scripts, to lock down a computer, or to prevent unwanted applications from running.

For more information about software restriction policies, see the Using Software Restriction Policies to Protect Against Unauthorized Software.

Limit Terminal Server Security Auditing

Auditing any system can introduce significant performance overhead depending on the number of events you audit and the number of user sessions that generate the events. When you configure a terminal server on Windows Server 2008, the cumulative effect of auditing events for multiple users working on the server at one time can affect the terminal server's performance.

In addition, for event logs to have any value you need staff to effectively review the logs on a regular basis. The more events you log, the larger the impact on performance and the more effort it will take to assess them.

For these reasons, Microsoft recommends to only enable as much event auditing that your organization can effectively use to balance security logging needs with the performance requirements of your terminal servers. In addition, you should test the impact of any changes to the terminal servers' auditing policies before you introducing an updated policy set to any production servers.

The following table identifies audit policy object names, audit setting descriptions, and recommended audit settings in Windows Server 2008.

Table 11.28 Terminal Server Audit Policy Settings

Policy object	Description	Recommended setting
Audit account logon events	This policy determines whether to audit each instance of a user logging on or off from a computer that is used to validate the account. Account logon events are generated when a domain user account is authenticated on a domain controller. The event is logged in the domain controller's security log. This policy is typically enabled only on domain controllers and is not normally required on a terminal server.	No Auditing
Audit account management	This policy determines whether to audit each event of account management on the terminal server. Examples of account management events include: • A user account or group is created, changed, or deleted. • A user account is renamed, disabled, or enabled. • A password is set or changed.	Audit Success and Failure
Audit directory service access	This policy determines whether to audit the event of a user who accesses an Active Directory Domain Services (AD DS) object that has a specified system access control list (SACL). This policy is typically enabled only on domain controllers and is not normally required on a terminal server.	No Auditing
Audit logon events	You can use this policy to audit each instance of a user logging on or off a terminal server.	Audit Success and Failure
Audit object access	This policy determines whether to audit the event of a user who accesses an object, such as a file, folder, registry key, printer, or any object that has a specified SACL. Because this policy can generate a large number of entries, Microsoft recommends to only use this setting to audit failures that indicate unauthorized users attempting to access objects.	Audit Failure
Audit policy change	This policy determines whether to audit each instance of a change to user rights assignment policies, audit policies, or trust policies on the terminal server. Because this data should rarely change, Microsoft recommends to audit these changes.	Audit Success and Failure

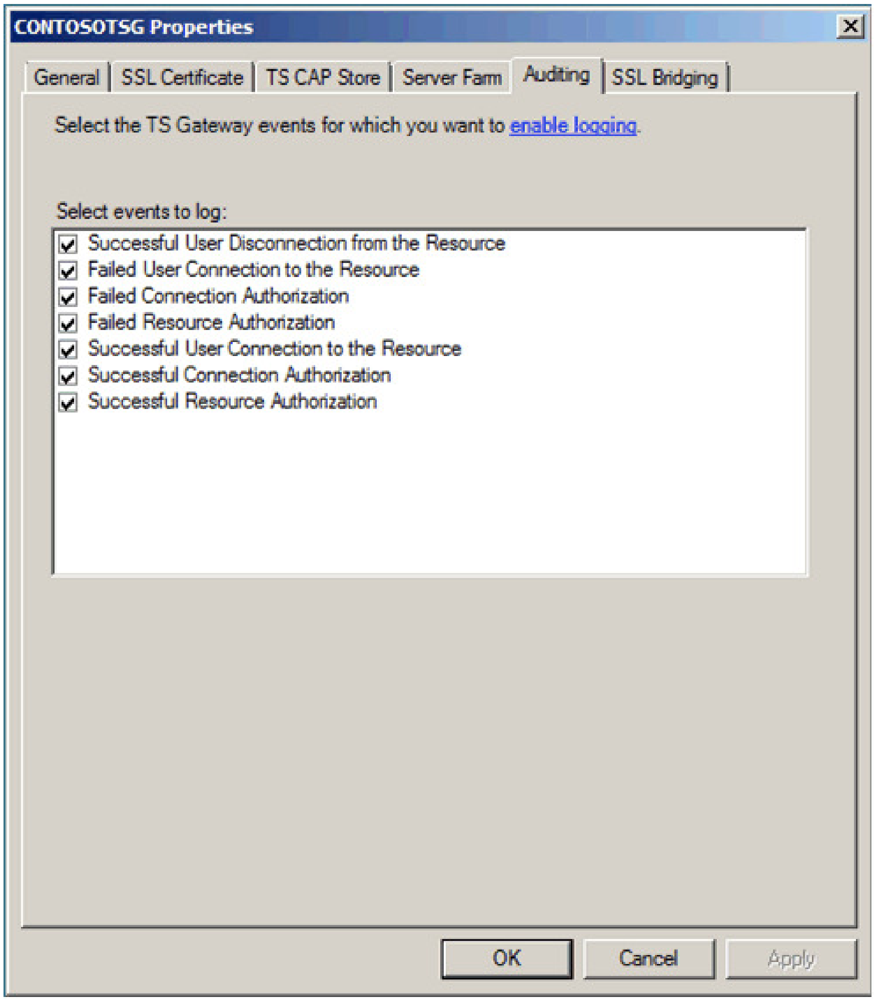
Policy object	Description	Recommended setting
Audit privilege use	This policy determines whether to audit each instance of a user exercising a user right. This policy can also generate a large number of entries in the security event log. For this reason, Microsoft does not typically recommend to log successful events for this policy because the event volume is likely to slow the performance of the terminal server.	Audit Failure
Audit process tracking	This policy determines whether to audit detailed tracking information for events, such as program activation, process exit, handle duplication, and indirect object access.	Audit Failure
Audit system events	This policy determines whether to audit users when they restart or shut down the computer or when an event occurs that affects either the system security or the security log.	Audit Success and Failure

After enabling any of these audit settings, it is important to check the event logs on the terminal server regularly and archive them as needed. If you choose to enable the **Audit object access** setting, you also need to configure auditing on each object that you want to track. Microsoft recommends restricting this capability to a manageable number of objects.

In addition to the ability to audit file system and registry objects, terminal servers can also report audit information about terminal server connections. These auditing reports record actions attempted during user sessions. For example, you can monitor actions such as modifying connection properties or remotely controlling a user's session after enabling connection auditing.

To enable Connection Auditing

1. On the terminal server, click **Start**, click **Administrative Tools**, and then click **Terminal Services Configuration** to open this tool.
2. In the right-hand panel, under the **Connections** list, right-click the desired connection name (**RDP-Tcp** by default), and then select **Properties.**
3. In the **Properties** dialog box, click the **Security** tab. If a **Terminal Services Configuration** information dialog box pops up, click **OK**.
4. Click the **Advanced** button, and then select the **Auditing** tab.
5. Click the **Add** button, type the name of the user, computer or group that you want to audit, and then click **OK**.
6. Select the seven audit policies as indicated in the following figure.



Select the TS Gateway events for which you want to enable logging.

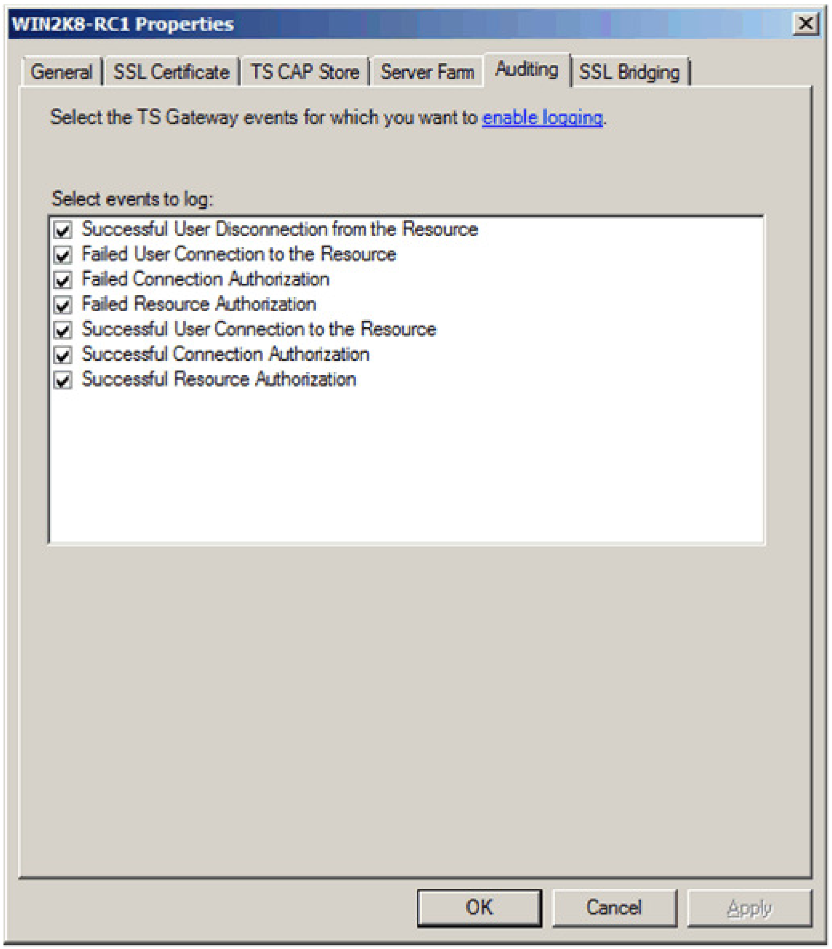
Select events to log:

☑ Successful User Disconnection from the Resource
☑ Failed User Connection to the Resource
☑ Failed Connection Authorization
☑ Failed Resource Authorization
☑ Successful User Connection to the Resource
☑ Successful Connection Authorization
☑ Successful Resource Authorization

Figure 11.2 Terminal Server Connection Audit Entry Options

The seven entries listed in the previous figure can be useful when checking for security issues on a terminal server. Typically, only a system administrator should attempt both the "remote control" and "logoff" actions on another session. If attempts for these actions occur from a standard user account, this could indicate unwanted user behavior and require further investigation.

There are also a series of events specific to TS Gateway. By default all of these event types are audited. You can use TS Gateway Manager to specify the types of events that you want to monitor, such as unsuccessful or successful connection attempts to internal network resources (computers) through a TS Gateway server. You also can configure what event types to audit by right-clicking the server you want to manage in TS Gateway Manager, and selecting **Properties**. Then in the **Server Properties** dialog box, click the **Auditing** tab.



Select the TS Gateway events for which you want to enable logging.

Select events to log:

☑ Successful User Disconnection from the Resource
☑ Failed User Connection to the Resource
☑ Failed Connection Authorization
☑ Failed Resource Authorization
☑ Successful User Connection to the Resource
☑ Successful Connection Authorization
☑ Successful Resource Authorization

Figure 11.3 Terminal Server Gateway Auditing Options

For more information about TS Gateway event types, see TS Gateway Server Connections in the "Troubleshooting" section of the Windows Server 2008 TechNet Library.

Securing the TS Gateway

After you install the TS Gateway role service and configure a certificate for the TS Gateway server, you must create Terminal Services connection authorization policies

(TS CAPs), computer groups, and Terminal Services resource authorization policies (TS RAPs). These policies are required to ensure that the TS Gateway service functions correctly.

Although the Add Role Services Wizard for TS Gateway includes an option to generate a self-signed certificate, this selection is recommended only for testing and evaluation purposes. For your production deployment, Microsoft recommends to obtain a computer certificate from a trusted certificate authority (CA).

Microsoft recommends the following security-related configuration recommendations for the desktop environment on terminal servers. If you need help to complete any of the checklist items, see the following sections in this chapter for additional details and recommendations.

Table 11.29 TS Gateway Configuration Checklist

	Configuration tasks
	Use Terminal Services connection authorization policy (TS CAP).
	Use Terminal Services resource authorization policy (TS RAP).
	Secure TS Gateway IIS installation.

Use Terminal Services Connection Authorization Policy (TS CAP)

Terminal Services connection authorization policies (TS CAPs) allow you to specify who can connect to a TS Gateway server. You can specify a user group that exists on the local TS Gateway server or in Active Directory Domain Services (AD DS). You can also specify other conditions that users must meet to access a TS Gateway server.

For example, you can specify that all users who connect to a specific terminal server that is hosting a human resources (HR) database through a TS Gateway server must be members of the "HR Users" security group. You can also specify that the client computer that initiates the connection must be a member of an Active Directory security group in the corporate network to connect to the TS Gateway server. By requiring that the computer be a member of a specific Active Directory security group in the corporate network, you can exclude users who attempt to connect to the corporate network from kiosks, airport computers, or home computers that are not trusted.

For enhanced security when client computers connect to the internal corporate network through TS Gateway, you can also specify whether to disable client device redirection for all devices supported by the Terminal Services client, or for a specific type of device, such as a disk drive or supported Plug and Play devices. If you disable client device redirection for all devices supported by the client, all device redirection is disabled, except for audio and smart card redirection.

When you select the option to disable device redirection for specific device types or to disable all device types except for smart cards, the TS Gateway server will send the request back to the client with a list of the device types to be disabled. This list is a suggestion only; it is possible for the client computer to modify the device redirection settings in the list.

Caution Because the TS Gateway server relies on the client computer to enforce device redirection settings that the server suggests, this feature does not provide guaranteed security. Suggested device redirection settings can only be enforced for RDC clients. The settings cannot be enforced for client computers that do not use RDC. In addition, it is possible for a malicious user to modify an RDC client so that the client ignores the suggested settings. In such cases, this feature cannot provide guaranteed security, even for RDC clients.

In addition, you can specify whether remote clients must use smart card authentication or password authentication to access internal network resources through a TS Gateway server. When both of these options are selected, client computers that use either authentication method are allowed to connect.

Finally, if your organization has deployed Network Access Protection (NAP), you can specify that the client must send a statement of health (SoH). For information about how to configure TS Gateway for NAP, see "Configuring the TS Gateway NAP Scenario" in the *TS Gateway Server Step-by-Step Setup Guide* for Windows Server 2008.

Important Users are granted access to a TS Gateway server if they meet the conditions specified in the TS CAP. You must also create a TS RAP. A TS RAP allows you to specify the internal network resources that users can connect to through TS Gateway. Until you create both a TS CAP and a TS RAP, users cannot connect to network resources through this TS Gateway server.

Use Terminal Services Resource Authorization Policy (TS RAP)

Terminal Services resource authorization policies (TS RAPs) allow you to specify the internal corporate network resources that remote users can connect to through a TS Gateway server. When you create a TS RAP, you can create a computer group, or a list of computers on the internal network to which you want remote users to connect, and then associate it with the TS RAP.

For example, you can specify that users who are members of the "HR Users" user group be allowed to connect only to computers that are members of the "HR Computers" computer group, and that users who are members of the "Finance Users" user group be allowed to connect only to computers that are members of the "Finance Computers" computer group.

Remote users connecting to an internal corporate network through a TS Gateway server are granted access to computers on the network if they meet the conditions specified in at least one TS CAP and one TS RAP.

Note When you associate a TS Gateway-managed computer group with a TS RAP, you can support both fully qualified domain names (FQDNs) and NetBIOS names by adding both names to the TS Gateway-managed computer group separately. When you associate an Active Directory security group with a TS RAP, both FQDNs and NetBIOS names are supported automatically if the internal network computer that the client is connecting to belongs to the same domain as the TS Gateway server. If the internal network computer belongs to a different domain than the TS Gateway server, users must specify the FQDN of the internal network computer. Together, TS CAPs and TS RAPs provide two different levels of authorization that allow you to configure a more specific level of access control to computers on an internal corporate network.

Computer Groups Associated With TS RAPs

Remote users can connect through TS Gateway to internal corporate network resources in the following ways:

- **As members of an existing security group**. The security group can exist in Local Users and Groups on the TS Gateway server, or in AD DS.
- **As members of an existing TS Gateway-managed computer group or a new TS Gateway-managed computer group**. You can configure the TS Gateway-managed computer group by using TS Gateway Manager after installation.

A TS Gateway-managed group will not appear in Local Users and Groups on the TS Gateway server, and you cannot configure it using Local Users and Groups.

- **Using any network resource**. In this case, users can connect to any computer on the internal corporate network that they can connect to when they use Remote Desktop Connection. This option is not recommended because it expands the potential attack surface of your network.

Secure TS Gateway IIS installation

In high-security environments, to prevent authenticated users with valid password or smart card credentials from reaching the RPC layer, consider locking down the TS Gateway server by disabling IIS virtual directories. You can make the following modifications to the IIS installation to further decrease the attack surface of a TS Gateway server:

- Eliminate unneeded ports from the ValidPorts registry key.
- Disable password authorization in IIS for pure smart card deployments.
- Limit password authorization in IIS to only users who are should authenticate to the TS Gateway.
- Limit access to the RpcWithCert virtual directory to ensure that a username mapping has occurred in IIS.
- Remove unneeded CA root certificates from the Trusted Root Certificate Authorities store.

More Information

The following resources on Microsoft.com can provide you with more security best practice information about how to design and maintain a server running Windows Server 2008 that performs Terminal Services:

- "How to change Terminal Server’s listening port": Microsoft Knowledge Base article 187623.
- Technical Reference Terminal Services for information about Group Policy settings.
- Terminal Services in the TechNet Library.
- The "Working with Quotas" section of the *Step-by-Step Guide for File Server Resource Manager*.
- *TS Gateway Server Step-by-Step Setup Guide*: "Configuring the TS Gateway NAP Scenario" section.
- Using Software Restriction Policies to Protect Against Unauthorized Software .
- Windows Server 2008 TechNet Library.
- Other Terminal Server and Virtualization-related Solution Accelerators:
  - Introduction to the Infrastructure Planning and Design guide series.
  - Microsoft Assessment and Planning Toolkit Solution Accelerator (MAP).
  - Microsoft Deployment Solution Accelerator, which is the next version of Business Desktop Deployment (BDD) 2007.
  - *Windows Vista Security Guide*.